Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Bjørn Inge Sletta

Overview of Data Protection status in European Lotteries and Recommendations towards a Better Practice

Masteroppgave i Informasjonssikkerhet
Veileder: Bian Yang
Juni 2021

NTNU
Kunnskap for en bedre verden

Bjørn Inge Sletta

Overview of Data Protection status in European Lotteries and Recommendations towards a Better Practice

Masteroppgave i Informasjonssikkerhet
Veileder: Bian Yang
Juni 2021

Norges teknisk-naturvitenskapelige universitet
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU
Kunnskap for en bedre verden

NTNU
Norwegian University of
Science and Technology

Overview of Data Protection status in European Lotteries and Recommendations towards a Better Practice

Author(s)
Bjørn Inge Sletta

Master in Information Security MISEB
30 ECTS
Department of Information Security and Communication Technology
Norwegian University of Science and Technology,

31.05.21

Supervisor Bian Yang

Sammendrag av Masteroppgaven

Tittel:	**En studie av personvern i Europeiske lotterier med forslag til forbedringer av dagens praksis**
Dato:	31.05.21
Deltakere:	Bjørn Inge Sletta
Veiledere:	Bian Yang
Oppdragsgiver:	Norwegian University of Science and Technology
Kontaktperson:	Bjørn Inge Sletta, bjorn-inge.sletta@bbnett.no, 95981426
Nøkkelord:	
Antall sider:	86
Antall vedlegg:	1
Tilgjengelighet:	Åpen

Sammendrag:

Summary of Graduate Project

Title:	**Overview of Data Protection status in European Lotteries and Recommendations towards a Better Practice**
Date:	31.05.21
Authors:	Bjørn Inge Sletta
Supervisor:	Bian Yang
Employer:	Norwegian University of Science and Technology
Contact Person:	Bjørn Inge Sletta, bjorn-inge.sletta@bbnett.no, 95981426
Keywords:	
Pages:	86
Attachments:	0
Availability:	Open

Abstract:

Preface

This master thesis is written as the final part of a 3 years part time study in 'Experienced based master in Information security' at NTNU. During the last three years I have studied a number of subjects related to information security, and as a final part I have chosen to focus on data protection and privacy in European lotteries, both relevant from a personal point of view and my daytime job as Data Protection Officer at Norsk Tipping. The finale work will give a deeper understanding of risks related to transparency for handling of personal data and techniques that could be used to ensure such transparency for both data subject and data controller.

My believe is that privacy, data protection and data transparency is not only is a question of compliance with Laws and Regulations, but also could be a business advantage for data handlers that both manage to handle personal data lawfully and at the same time reflect this to the users of their services. For the Lottery Business it will be of specific importance to show transparency towards winner selection, prize calculation and responsible gaming tools(Gaming limits) towards both customers and national authorities. The presented material will also be relevant outside the lottery business since all data processors within the EU need to conduct their operations in compliance with GDPR.

My Supervisor has been Bian Yang, and I would like to thank him for his contribution and guidance during the last months of work.

1 Abstract

In this master thesis we present a comprehensive study of practice related to privacy and handling of personal data in European lotteries. The study aims to document how the GDPR framework is understood and implemented across lotteries in Europe and identify differences between status and expectations in important laws and standards.

In addition to GDPR, Important Information Security Standards like the ISO 27000 series will be presented together with important EU regulations, lottery specific security standards and privacy concepts.

Using questionnaires, inspection of web sites and automated analysis we collect a substantial amount of data related to important fundamental data protection rights in European lotteries.

By analysing the collected material important techniques for data protection and data transparency is identified. Presented research material documents how they are implemented in European lotteries and shows significant variations between the different Lotteries. The thesis discuss the findings in the collected material and suggests how the described techniques can be implemented to be both GDPR compliant and support a healthy company reputation.

Anonymous gambling products will not be a part of this study, and I will not make any attempt to investigate identification of anonymous ticket holders or prize winners. From a security and compliance perspective this could be very interesting since these products are known to be closely related to money laundry and criminal activity, but the scope of this thesis is related to data protection and use of personal data and the understanding of GDPR.

Contents

List of Figures

2 Introduction

When the General Data Protection Regulative GDPR was introduced to all member states in the EU and EEA in 2018, it did not just introduce a common understanding and regulation of data protection in Europe, but also new and changed requirements for many organizations that handle personal data. A whole set of new regulations where made applicable for different business operations who traditionally have had limited concerns or knowledge about data protection and privacy. The lottery and gaming business who traditionally have offered anonymously gambling products and non disclosure of personal data typically would have to implement extensive techniques for both collection, use and storage of personal data. A valid legal basis for handling of personal data became now mandatory, and a comprehensive customer contract needed to be presented with references to data protection policies or even national law.

An increased requirement for compliance with national gambling regulation, anti money laundry and and data protection has changed the gambling industry from limited or no handling of personal data to a long time relation with individual customers involving loss/bet limitations and transparency towards handling of personal data. Being compliant with GDPR and data protection requirements is of specific interest since companies and industries with a high cash flow could risk substantial fines up to €10 million, or 2 percent of the firm's worldwide annual turnover.

Increasing privacy concerns from customers is also important. A company reputation could take years to build, but a single incident could be devastating if we fail to handle data protection and personal data wisely and lawful.

The response from the gambling industry has been to use traditional techniques as increased access to customer data and comprehensive data protection policies, but still we see a gap between expectations in laws and frameworks and implemented techniques. Data protection policies and customer contract could both be hard to read and understand, and collection of personal data with 3. part tools as cookies could be both used unwisely and even in violation with law.

The objective with this master thesis is to document the practice in European lotteries and identify this gap between law, standards and even ethics related to data protection, privacy and handling of personal data. There is a need to both identify these gaps an recommend how they can be closed. This will ensure that collection and use of personal data is done both wisely and in accordance with law an important information security standards.

3 Important laws and frameworks

Several laws and regulations is related to the use and collection of personal identifiable information(PII) and data transparency. The most important law for Norway and Europe is by far the General Data Protection Regulation(GDPR)[1], but data transparency meaning access to individual personal data at different levels is also reflected in online business regulations like bank services or retailer services. The PCI DSS standard (Payment Card Industry Data Security Standard)[2] typically states that information about handling of PII is required to be documented and informed to the individual users.

Other technical standards like ISO27001/27001 and the ePrivacy[3] directive is also important. In this initial part of the text I will be focusing on the theoretical basics of data protection and transparency identifying the most important laws and regulations that we need to both understand and comply to.

3.1 GDPR

The General Data Protection Regulation (GDPR)[1] was adopted by the EU countries in 2016 and made enforceable for all EU and EEC countries in 2018. In Norway the regulative was introduced in 2108 (Lov om behandling av personopplysninger (personopplysningsloven[4]) the same year. The regulation replaces existing regulations within EU and introduces a common understanding of data protection and data transparency among the member countries. Before GDPR there was a significant difference among the member states causing both unequal treatment of cross-country business operations and individuals. The law comes with a mechanism to handle infringements with fines up to 10 million Euros or 2 percent of revenue, making non compliancy a costly mistake. Such fines have been seen in several countries making it likely that national data protection agencies will monitor the use and collection of data closely. The law also states that the character of personal identified data involved should be taken into account (art. 83), making it likely that data processors handling sensitive data and large data sets should be specifically aware of the impact of the regulation

The 7 important principles of GDPR are:

- **LAWFULNESS, FAIRNESS AND TRANSPARENCY:** Data should be obtained in a lawful manner. For most data processors this will involve the use of contract or consent from the data subject.
- **PURPOSE LIMITATION:** Data can only be collected for those purposes that has been clearly communicated to the data subject
- **DATA MINIMISATION:** A minimum of data to perform the agreed purpose int the contract or consent should be collected
- **ACCURACY:** Collected data should be kept both accurate and up-to-date. Old and outdated data should be deleted.

- **STORAGE LIMITATION:** Personal identifiable data should not be kept longer than agreed on with the data subject.
- **INTEGRITY AND CONFIDENTIALITY(security):** Data should be collected and stored in a way that ensures optimal confidentiality, integrity and availability.
- **ACCOUNTABILITY:** GDPR requires that processes involving collecting and storage of personal identifiable data is documented and could be presented to authorities to document compliance

Art. 4 defines personal identifiable data as any information relating to an identifiable person. Both court practice and legal definition has elaborated this to involve geographical data, dynamic IP addresses and bio metric data. Both Datatilsynet[5] and the Information Commisioners Office[6]in the UK as a comprehensive description of different data types on their home pages.

Specific precautions should be evaluated regarding data transfer in/out of EU since GDPR not automatically relates to national legislation's, typically Privacyshield[7] in the US. The Privacy Shield Framework were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to ensure that transfer of personal data were done according to law and regulations. As a result of the SchremsII[8] lawsuit in 2020, appropriate safeguards now has to be introduced before transfer of PII to the US involving a specific risk assessment for the transfer.

Like any other organization or industry handling Person Identifiable Data(PII), the lottery and gambling industry will have to be compliant with GDPR. Some lotteries operating in typical northern Europe have collected and used PII for many years offering registered gambling etc. while other lotteries traditionally have offered anonymously gambling and might have a longer way to go to be compliant.

3.2 ISO 27001

ISO 27001[9] is a comprehensive security standard including a number of recommended controls and requirements. The described controls are both operational controls presented as best practice to handle information securely (Annex A), and an approach to establish, implement, maintain, and continual improve a system for security management. (ISMS - Information Management System). ISO 27001 and related standards ins the ISO 27xxx series is highly relevant for the gambling industry :

- Certifications could be mandatory for participation in major multinational lotteries
- Certification and compliance level could be a part of procurement processes as basis for both qualification and evaluation of tenders.

The requirements are generic, meaning that they easily could be adapted and introduced to any organisation. An organization could choose to certify against ISO 27001 by using an external approved auditor. ISO 27001 is by far also the most important security standard in Europe.

Like other ISO standards ISO 27001 uses the PDCA cycle (Plan - Do - Check - Act) to align

the activities needed to comply with the standard:

- **PLAN:** Establish a plan through policies, guidelines etc. describing the objectives and wanted results
- **DO:** Implement the plan
- **CHECK:** Measure the performance against described objectives
- **ACT:** Corrective and preventive actions to ensure that non-conformity's is handled correctly

Other standards like i.e. NIST 800-12[10] could be an alternative, but since ISO is by far the most used information security standard in Europe this will be used as an example. NIST 800-12 is typically used by organizations in Northern America.

3.3 ISO 27005

ISO 27005[11] is another standard in the ISO 27000-series providing best practice for management of risks related to information security. The standard is a natural extension of ISO27001 providing a risk based approach to maintain and monitor the controls in this standard. This should be done involving a set of activities like:

- **RISK MANAGEMENT:** Establishing a risk management context like risk identification, ownership and risk calculation
- **RISK ASSESSMENTS:** Establishing a risk assessment process with identification of assets, threats, vulnerabilities etc.
- **RISK TREATMENT:**Risk treatment(Avoid, modify, share or retain risks)
- **RISK ACCEPTANCE:** Definition of risk acceptance criteria
- Communication and information sharing related to risk
- **RISK MONITORING:** Risk monitoring and review

Annex C and D describes typical threats/vulnerabilities related to personal data and risk/treat assessments

There is a close relation between the ISO 27000 standards and GDPR since handling of personal data should involve risk assessments and identification of possible risks at some stage. A risk based approach is specifically described in GDPR art. 32 where level of security is to be set appropriate to related risks.

3.4 ISO 27701

ISO 27701[12] is an extension to ISO 27001 with additional requirements and controls related to data protection and secure handling of personal identifiable data. Guidelines for implementation of every article in the GDPR is provided. This is presented as a set of additional controls easily adaptable to an existing ISMS(Information Security Management System).

3.5 Privacy and Electronic Communications Directive (ePrivacy directive)

The Privacy and Electronic Communications Directive (ePrivacy directive)[13] is an EU directive from 2002 intended to regulate important issues like data protection and privacy in electronic communication. Together with the GDPR regulative it creates the legal basis for privacy and lawful handling of personal identifiable data within the EU. The original directive from 2002 is amended by a new and revised version in 2009 introducing several changes related to the use of prior consent, cookies and treatment of communication data. The ePrivacy directive regulates the use of 'cookies' and 3 part tracking mechanisms making it important for any lottery or gambling operator that utilize these kind of tools.

3.6 The Ekom law

The Ekom law[14] is a national law legislation in Norway. As an EEC country Norway has introduced the ePrivacy directive[13] to answer the regulations in the directive by introducing the Ekom law in 2003. As stated in the EU directive this specific regulation is pt. important regarding the use of 'Cookie technology' and ecetronic traffic data.

Articles 2.7 B is off particular interest since it reflects the ePrivacy directive and states that prior consent is needed for cookies and information trackers used by operators in Norway

3.7 WLA-SCS

The WLA-SCS[15] is a security and control standard developed and maintained by the World Lottery Association (WLA). The standard defines a number of lottery specific security controls strongly related to generally accepted information security and quality terms. Important controls are related to the handling of winner information, draw security and handling of instant tickets etc.

Lotteries can choose to certify to the standard and achieve a WLA-SCS certification. WLA-SCS is typically implemented in an organization as a part of a company ISMS system with ISO 27001 controls. A WLA-SCS certification is not only mandatory for participation in international lotteries like VikingLotto or Eurojackpot, but it will also document compliance with best practice for lottery operations.

4 Privacy concepts and theoretical models related to lotteries and gambling industry

Most cultures, both existing and extinct civilisations acknowledge the fundamental right to keep some parts of their life hidden or protected from a wider society. In its simplest form it could be to keep the door to your home or residence closed while more complex regulations could be laws and regulations reflecting expected behaviour and possible penalties for non-compliancy. For some individuals like slaves or prisoners this could off course be hard to see, but it also reflects the removal of fundamental human rights.

Individual privacy rights is more related to western cultures where the first traces of something that could be referred to as a privacy theory could be found in USA in 1890 where Samuel D. Warren and Lois Brandei argued that it should be a right to be left alone in a article called 'The right to privacy'[16]

The right to privacy was adopted by the Universal Declaration of Human Rights in 1948, while the first national data protection law was introduced in Sweden in 1973. In Norway the right to was adopted in section 102 of the constitution in as early 1814 with inspiration from both France and the US legislation's. During the 1970, 1980 and 1990 we saw a rise of national data protection laws as result of increasingly more advanced computer and network systems.

In later years we have seen the rise of trans national regulations resulting in the EU GDPR regulations[1] and the Privacy Shield[7] for cross Atlantic data transfer to the USA even though the country still is missing a comprehensive national law for data privacy. Reported privacy concerns has raised to new heights in the last years, and the privacy shield has been challenged by several privacy groups including the European Court of Justice who determined that it was inadequate in the SchremsII[8] decision earlier this year. Under Privacy Shield data transfer was done according to contract as stated in GDPR article. 45, while businesses now have to conduct a specific risk assessment to ensure that a sufficient protection level can be met. (*adequate safeguards and on conditions that individuals are provided with enforceable rights and effective legal remedies*)

4.1 Privacy

Privacy could be defined as the right of individuals to control over personal information as described by Alan Westin in his fundamental work 'Privacy and freedom' from 1967[17], and later by the American jurist and lawyer Charles Frieds in his book 'Privacy'[18]. Westin details this by arguing that each individual should be able to determine which information about himself or herself should be known by others, while Frieds elaborates privacy as the control we have about ourselves. Both definition are still essential even though the concept of privacy

have been increasingly challenged by both new technology and extensive use of personal data. Alan Westin defined four states of privacy, solitude, intimacy, anonymity, and reserve. Several studies like Koops et. al.[19] suggest that new and more comprehensive models is needed. A more modern and contemporary version is typical defined by the Australian law reform commission[20] as:

- **INFORMATION PRIVACY:** Handling and regulation of personal data like credit data, health data etc.
- **BODILY PRIVACY:** Protection of individuals against physical procedures like genetic testing, random search by police/authorities etc.
- **COMMUNICATION PRIVACY:** Security for personal communication like mail and telecommunication
- **TERRITORIAL PRIVACY:** Physical limitations like boundaries/limitations at work of public space including ID checks, CCTV surveillance etc.

In this text I will mainly focus on Information privacy and communication privacy.

4.2 Privacy and data protection

Several models for privacy and data protection exists, many of them widely discussed and explained as either having a technological approach like ISO 27001/27701 or lawfulness like the GDPR. EPIC(Electronic Privacy Information Center) published a comprehensive study as early as 2007 where they defined four models for effective privacy protection[21]:

- **NATIONAL LAWS:** National laws and regulation related to privacy and the protection of personal data, typical national data protection laws as the EU GDPR
- **SECTORAL LAWS:** Law and regulations that aims to regulate privacy for certain sectors, typical the financial sector(credit information) and internet privacy like the use of cookies etc. A typical example could be the 'Ekomm directive' in Norway[14]. In international context ISO 27001(information Security management) or the extension ISO 27701(Privacy information management) are highly relevant standards
- **SELF REGULATION:** Various form of self-regulative frameworks could be established within companies and industries to encourage self-policing. This is perhaps the least developed model since business standards seems to favour business needs and lack enforcement and protection of data. A typical example could be IAB and TCF (Transparency and Consent Framework)[22] that aims to develop a framework for consent management for the advertising industry.
- **TECNOLOGIES OF PRIVACY:** With the development of new and improved functionality in web browsers and digital communication channels we have seen a development of user dependent technology making it possible for the individual user to enforce privacy protection. Typical examples could be Ghostry who makes it possible for users to block tracking cookies and encryption, anonymous browsers like TOR, block chain technologies etc.

4.3 The APCO model

So far we have seen that bot theoretical models and frameworks seems to focus mostly on data protection, and not necessarily data transparency. Initially I argued that it could be a

business advantage to implement data transparency, and that the lack of transparency could be a threat to company reputation. To fully understand the difference between data protection and transparency we need a closer look at the theory behind both data protection and transparency and see how we can categorize the different techniques we find in data protection laws and how they are implemented, or at least identify the intention behind the regulations.

Smith[23] defines privacy concern as a relation between a set of independent and dependent variables in the APCO model(Antecedents – Privacy Concerns - Outcomes) as shown in Figure 1.

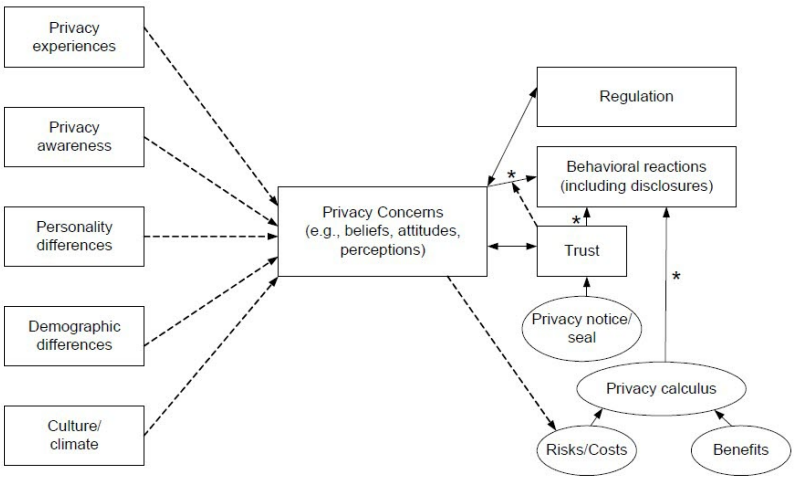


Figure 1: The APCO model

Smith argues that individual characteristics strongly will affect concerns related to privacy. Important independent variables is identified as:

- **PRIVACY EXPERIENCE:** Abuse of personal data. Individuals that have experienced abuse of personal data tend to be more aware of privacy than others
- **PRIVACY AWARENESS:** Information about privacy practice related to collection of data will give increased privacy awareness
- **PERSONAL DIFFERENCES:** Individuals with high social awareness are more aware of privacy issues than others.
- **DEMOGRAPHIC DIFFERENCES:** Specific demographic groups tend to be more aware of privacy than others. Women are more concerned than men, poor or less educated are less aware than highly educated groups with higher income.
- **CULTURAL DIFFERENCES:** Specific societies could have weaker institutional trust and have a stronger relationship between potential risk and privacy concerns

Important dependent variables are defined as:

- **REGULATION:** If individuals find that their privacy is not sufficient protected by data handlers they will prefer state regulations with a possibly regulatory response.

- **BEHAVIOURAL REACTIONS:** Individuals willingness to disclose personal information. Trust could also be argued to be a meditating variable closely related to individual reactions.
- **PRIVACY CALCULUS:** Consumers or individuals will perform a risk/cost analysis to analyse the outcome they will face when disclosing personal data. Privacy risk will be the believe of a high potential loss or negative consequences, while privacy benefit will be the believe of a favourable outcome like financial reward, personification and social adjustment benefits.

Dependent variable are depending or related to independent variables meaning that changes or characteristics like privacy experiences can explain behavioural reactions. Researchers like Eastclick[24] and Metzger[25] shows trust as a meditating variable between privacy concerns and disclosure of information. Firms that are able to show or create trustworthiness related to privacy are more likely to have customers less worried about privacy concerns than other companies. Consumers who trust a company are more willing to share their personal data and have a competitive advantage compared to their rivals.

A typical example of trust related to disclosure of personal data is collection of consent for personalization where individuals tend to be more unwilling to share personal data than perhaps any other place. A typically answer rate according to Vernet et al.[26] could be 50 percent in user surveys. This number is not directly transferable to the collection of consent for marketing purposes who might even be lover, but it indicates that far from everyone would give their consent to this kind of activities. When Norsk Tipping launched their consent management platform for personalization in 2019 a total of 723.000 out of 740.00(98 percent) who were exposed to this question gave their consent. An explanation to this astonishing high number is the reputation Norsk Tipping has in the population in Norway. The company is rated as number 12 related to reputation i Norway by Kantar[27]. Among the participants in the survey 97 percent stated a high level of trust to the company.

These numbers shows a clear connection between disclosure of personal data and trustworthiness, but at the same time it shows that the potential loss of trustworthiness is also very present. Any damage to reputation caused by loss or misuse of personal data could be devastating to company reputation resulting in less company trust and unwillingness to disclose personal data.

4.4 Trust and trustworthiness

Mayer et al[28] defines trustworthiness or characteristics of a trustee responsible for trust with three characteristics:

- **ABILITY** - Skills or characteristics that enables a part to have influence within a domain
- **BENEVOLENCE** - Is the believe that a trustee want to do good to the trustor
- **INTEGRITY** - Refers to the trustor's understanding that the trustee acts within a set of principles or rules that the trustor can find acceptable

Perceived trust will be the function of all three factors, and Mayer argues further that integrity will be the most important issue early in a relationship while perceived benevolence will have increasingly effect over time. Risk is also an essential component in trust building since engagement in a trusting action involve a certain level of risk. The context in which the risk is taken is also of importance since the consequences of trust will be set by factors such as stakes involved, the balance of power and alternatives available for individual who gives trust.

If we transfer this theory to handling of personal data and transparency it is easy to argue that building trust in this context will be strongly connected to control and access to personal data, and that the data handler clearly states his intentions and acts within a predefined set of rules like GDPR etc. A study performed by Cisco[29] quantifies that a number of business advantages related to data privacy and data transparency. According to this benchmark study data breaches are less likely, and will a have less impact to business operators that shows a high level of privacy maturity. These findings are supported by Martin et al.[30] who finds that companies who fails to give customer access to their personal data or explain their privacy policies have a greater risk of financial harm than other companies after a data breach. These findings should be possible to relate the lottery and gaming industry where we will find examples and data in this study, but there will be other effects both mentioned in these studies a.o. like:

- A more effective market communication since improved insight in customer data will make it possible to personalize market communication if the customer gives his consent to this kind of profiling.
- More accurate, safe and structured data since GDPR has strict requirements for data safety and access to data(Confidentiality Integrity and Accessibility)
- Improved basis for decision making as a result of a higher data quality

Traditionally gaming and lottery operators operate in a market where trust and confidence tends to be low. This is strongly supported by Pallesen et al.[31] who finds that the population in Norway have week negative attitudes related to gambling. Customers seems to associate gambling with money laundry, match fixing and other more or less illegal actions making data transparency important to improve their trustworthiness. Other operators are more or less monopolists with a high level of trust among their customers making transparency important to maintain this position and even defend it against illegal operators who will try to challenge this situation.

4.5 Learning models in gambling

The basic concept of classical learning model is that gambling is a behaviour acquired as a interaction between internal and external factors. The cognitive behavioural model is one of the best developed learning models assuming that behaviour is an result of imitation, observational learning, reinforcement and cognition. Cognitive distortion is recognized as a misconceptions of reality, related to gambling typical underestimating consumed time spent on gambling, total amount of money spent, total loss etc. as described by Michael Auer[32]

The cognitive diamond as seen in Figure 2 is a common tool used to explain how different factors influences our daily life and situation behaviour, cognition is the way we experience the world through thoughts, feelings, bodily reactions and behavior. Cognitive behavioural ther-

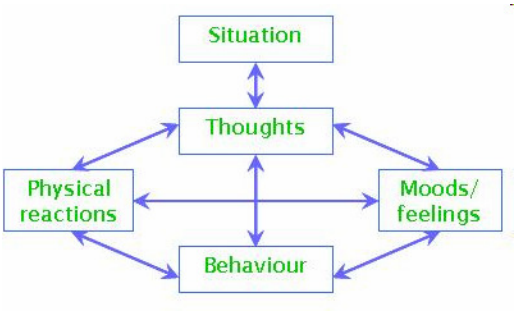


Figure 2: The cognitive diamond

apy is recognized as a highly effective treatment of gaming addiction by Hedman et al.[33] a.o.. Martens et al[34] studies shows that just receiving some kind of a personalized feedback about your gambling behaviour will have a positive impact on subsequent gambling. Typical tools used for normative feedback(alignment with gaming limits, social expectations etc.) related to gambling problems is:

- Self observation through access to gaming transactions
- Summary reports on used time, stakes, losses etc.
- Self diagnostic tools to raise self awareness

Lottery operators that offers this kinds of feedback relies on behavioural tracking by using either company specific tools/reports or commercially available tools like Neccton[35] or Playscan[36]. These kind of tools not only provide customer profiling based on gambling transactions, but also has the ability to produce personalized feedback and to some extent even produce projected values as feedback. Most lotteries also has mandatory registration for individual player accounts after the introduction of GDPR in 2018, making it possible to produce a individual profile for each player. Michael Auer[32] even argues that behavioural tracking will increase trust since it reflects transparency to regulators and gaming regulations etc. and states that the responsibility of the operator is to provide valuable information to support the player's decision making process, i.e an informed choice.

Considering GDPR[1] art. 4 that defines personal data as *any information relating to an identified or identifiable natural person*, this kind of feedback and behavioural tracking is to be considered as personal data. It can even be argued that information related to gaming prob-

lems and addiction is to be considered as health data as described in art. 9, and as a result of this will require a increased level of protection and a appropriate security(GDPR art. 32). This is supported by the National Data Protection Authority in Norway(Datatilsynet) who states that *information about player behaviour in specific situations could be health data...* in their answer to the suggested changes in the national gambling legislation in Norway in 2020[5] On the other side it can be argued that no diagnose is made, and that players with indications of gaming addiction is referred to medical expertise for further follow up.

I will not investigate the legal assessments in this document any further except to recognize the requirements in the GDPR regarding personal data and requirements related to correct handling. It is though important that GDPR art. 35(2)(a) requires data controllers to conduct a privacy impact assessment(PIA) any time *"a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person."*.

It will be of great interest though to investigate if lottery operators in Europe perform this kind of behavioral tracking and supply their customers with feedback, and the survey will have specific questions related to this matter.

4.6 The RENO model - How to understand responsible gambling principles

The RENO model presented by Blaszczynski et al[37] in 2004 describes a science based framework for principles related to responsible gaming. The model present two fundamental principles:

- The ultimate decision to gamble resides with the individual and represents a choice.
- To properly make this decision, individuals must have the opportunity to be informed.

These principles states as a guide for adoption and implementation of responsible gaming and initiatives to minimize the negative impact of gambling. Negative impact from gambling is recognized as addiction, financial problems etc. in a great number of studies, and needs no further presentation.. Blaszczynski strongly argues that the providers of gambling products must disclose and provide consumers with information that permits them to make informed decisions about their play, and their chances of winning. At the same time this information should both be relevant, objective and evidence based. Auer[32] pursues Blaszczynskies theory and and states that this should be done by providing valuable information to the player to support his decision making process(informed choice). Related to gaming problems these tools are commonly referred to as responsible gaming tools(RG tools). The most used RG tools used by online lottery operators is:

- **SELF EXCLUSION** where player voluntarily chooses to exclude himself from gambling for a period of time. Some operators also practice 3. part exclusion where players as excluded by the operator as a result of personal behaviour or personal bankruptcy, being a receiver of social security etc.
- **LIMIT SETTING**(Voluntary or mandatory) such as bet limits, loss limits and play limits either mandatory or set by governmental regulation

- **PERSONALIZED** feedback given to the player as a result of his player history, typical loss reviews, used time on gambling reviews etc. Some operators even practice the use of pop up message after spending a certain amount playing slot machines on line etc.

There is a close connection between the RENO model and fundamental data protection rights like access and control with personal data. Bonello[38] not only recognizes loss calculations as preventive tools, but also present this as a effective way to evaluate the effectiveness of responsible gaming measures. To be effective for both customer/player and operator of lotteries etc., a high level of transparency is needed to present the player with the opportunity to access these data and make his own decisions related to gambling.

This theory will be further investigated in this study were access to customer data like loss/-bet limits and personalized feedback like spending summary will be investigated.

Relevant information about collection and handling of personal data is also important at an initial state where a decision about being a customer or not is being made. Important issues that will be investigated is typical the presence of a data protection policy, customer contract etc.

4.7 Privacy Enhancement techniques(PET) and Transparency Enhancement techniques(TET)

The APCO model defines a relation between privacy awareness and collection of data. Collection of data is closely related to implemented techniques and processes for disclosure of personal data. To be trusted this must be done both securely and in accordance with data protection principles. Techniques that complies with these demands is often referred to as PET(Privacy Enhancement Techniques), or technologies that are designed for supporting privacy and data protection. This is a common terminology adopted by ENISA(The European Union Agency for Network and Information Security), and widely used by national data protection authorities like Canada[20] and Denmark[39]

PET is intended to be used to protect personal data by implementing tools and techniques like

- **CONSENT OR CONTRACTUAL AGREEMENT** when personal data is disclosed to a trusted third part. A contract or consent will then regulate further use of data
- **DATA MINIMIZATION** to ensure that only a minimum of data is collected. This could be done by only allowing certain types of data to be entered in a GUI
- **DEPERSONALIZING** by using techniques like TOR or nicknames etc. This could also only offer a certain or partial grade of anonymity since features like IP addresses and nicknames could be traceable back to its origin
- **CONTROL MECHANISMS** that allows users to exercise control over who should be entitled to receive and/or handle their personal data. PIMS(Personal Information Management System) offers this kind of functionality by letting data owners decide who and how their personal data could be shared. This could i.e. be consent management platforms like 'Tealium' or 'Google Ad manager' who offers the possibility to give to consent for personalizing across both sites and platforms.
- **TECHNICAL ENFORCEMENT** through access control, VPN tunneling, encryption etc.

that typically could ensure secure access to private data sets
- **PSEUDONYMIZATION** where information that could be traced back to one specific individual is replaced by 'pseudonyms' This allows analyzes to be run om data where the privacy for individuals is protected

PET technology more ore less reflects traditional data protection principles like lawfulness and technical security as as stated in GDPR and security frameworks like the ISO27000 series or NIST 800-12. To achieve transparency an extension of these tools is needed to provide individual information about details concerning personal data for individual data owners. Several researchers like Janic et al.[40] and Hedbom[41] refers to this as TET(Transparency Enhancement Tools) where information about how and where personal data is stored, data sharing with possible 3. part processing of data etc is offered to the individual data owner. Based on the research of Janic/Hedbom and personal experience the following classification of TET techniques is suggested:

- Tools that provide insight in intended data collection. This could be privacy statements and customer contracts with details concerning data storage, processing and/or data retention etc.
- Tools that provide insight in collected and/or stored data(ref. previous bullet point), but should also include information about sub suppliers and the use of data transfer agreements and the use of sub suppliers.
- Tools that provide insight in third part tracking, typical cookie statements with information about 3 part tracking cookies and/or the possibility to disable cookies
- Tools that provide insight into unintended data disclosure like data breaches reported to national data protection authorities.

The Lottery industry has adopted a number of typical PET and TET technology to protect personal data and provide transparency. Lotteries in this study typically have implemented techniques like:

- **CONTRACT** Customer contract, data protection policy and cookie policies to inform customers and possible customer about the collection and use of PII, the presence of behavioural tracking, sub suppliers etc.
- **CONSENT** Collection of consent for individual customer to allow marketing(profiling) and SMS/email communication ect.
- **SECURITY** Secure communication and use of secure methods for customer identification
- **DATA MINIMIZATION** Data minimization only allowing specific information to be entered
- **ACCESS TO DATA** Access to personal data through customer pages presenting collected PII. Some lottery operators even offer the possibility to export this data
- **ANONYMOUS DISCLOSURE** Anonymous disclosure of personal data to report suspect criminal activities related to money laundry and misuse of personal player accounts etc.

What we do not see is the presence of more advanced PET techniques like differential privacy or secure multi party computation etc, at least non of the participating lotteries revealed that such techniques were in use. This could be interesting to investigate further since this

kind of techniques could increase information security related to collection and use of PII, and possibly increase trustworthiness among customers and governmental agencies. Use of additional PET/TET will be further investigated as suggested recommendations in chapter. 8

4.8 The privacy paradox

The privacy paradox could be described as the discrepancy between the individual data owners intention to protect their privacy and how we actually behave when personal data is disclosed to on line sales channels etc. It seems like the concerns and risks we express not necessarily is reflected in our daily life's with profiles in social media, web stores or other online services where we freely provide personal data when this is required.

Studies like Wu[42] and Bake[43] not only recognize the privacy paradox as an explanation to human behaviour, but also argues that giving people control of personal data will increase their willingness to share their data, and that we are likely to see a privacy protection gap between users who understand why their privacy matters and those who don't. Bake's studies also shows that 'privacy fundamentalists'(Those who never give up online privacy) could be converted to 'privacy pragmatists'(Those who balance between data protection and benefits of data closure) by exposing them to reasonable disclosing arguments.

5 Definition of research question

Trough the presented theory we have seen a close relationship between privacy awareness and trust in online services. We have presented PET and TET techniques as tools to provide trust, but at the same time this is not the situation met by users of web services and sales channels. Many users report that data protection policies are either missing, hard to find or incomplete. Data could be collected for other purposes than expected ore even accidentally leaked or misused in criminal acts like ID theft or other kinds of misuse of personal data. This kind of observations related to data protection policies etc. is also supported by Wu[42] and Baeke[43] who argues that privacy information is both not very visible or/and at a technical high level making them inaccessible for users without this knowledge.

Further we have seen the presence of a privacy paradox where users express concerns about risks related to disclosure of personal data but still freely provide this kind of information when this is required. Baek argues that peoples opinion about online privacy is easily influenced by counterargument against sharing of data. This effect is more pronounced among people with low level of privacy knowledge as a privacy protection gap. There seems to be a mismatch between how data collectors explains the collection and use of personal data and how users of their services understand this information

If we relate this to the APCO model and theory presented in chapter 3, thrustworthiness is crucial to the disclosure of personal data. If the data object see benefits of disclosure and at the same time understands what principles and rules the data controller acts within, this will give the data object control of his personal data and increased the level of perceived thrust. A high level of trust will make it easier to collect consent for extended use of personal data and reduce the impact of data breaches as described by Martin[30], and reduce the risk of financial harm as presented by Cisco[29] in Chap. 3.

This hypothesis leaves us with a number of questions that either will be confirmed at least documented in real life studies and observations. The research question I will try to answer in this thesis is:

- What is the situation related to the use of TET and PET techniques in European lotteries, what kind of techniques are implemented and how.
- What are the differences between observations and expectations in laws, best practice/standards and ethics.
- What will be the best recommendations to improve the current situation

To answer these questions we need a representative collection of data from web sites. In this master thesis we will be using data collected from different lottery operators across Europe. Many of companies are operating as monopolists in a business many users relate to illegal money laundry and match fixing etc. making both keeping and building of trustworthiness important. By using questionnaires and manual inspection of data protection polices and cus-

tomer contracts etc. I will investigate the following topics closer:

What kind of TET technology is implemented by Lotteries in Europe?

- Privacy statements and customer contracts with details concerning data storage, processing and/or data retention etc.
- Insight in collected and/or stored data(ref. previous bullet point), but should also include information about sub suppliers and the use of data transfer agreements and the use of sub suppliers.
- Insight in third part tracking, typical cookie statements with information about 3 part tracking cookies and/or the possibility to disable cookies
- Insight into unintended data disclosure like data breaches reported to national data protection authorities and data subjects involved
- Lottery/gambling specific TET techniques like:
    - Voluntary Limit Setting
    - Self-Exclusion Schemes
    - Personalised Feedback
    - Win/loss amounts
    - Export of tickets

What kind of PET technology is implemented by Lotteries in Europe

- Lawfulness - Consent, contractual agreement or national law
- What kind of data is collected - Name, address etc,
- Data minimization
- Anonymous disclosure of data - i.e reporting of illegal activities related to money laundry
- Technical enforcement - Access control or other kinds of safe access to personal data
- Retention rules - How long is data kept by the data handler before deletion/anonymization
- Handling of data breaches - Information to customers and national data protection authorities

6 Methodology

To collect data to support the research question and analysis as presented i chap. 5 the following methods for data collection will be introduced:

- **Questionnaires**
  - To collect live observations and documentation of current practice
- **Manual observations of data protection policies and cookie policies etc.**
  - To collect data from lotteries not answering the survey
  - Collection of additional data not requested in the questionnaire
- **Automated inspection of web sites**
  - To reveal any bias between answers and actual observations like the presence of 3. part tracking mechanisms etc.
- **Focus group interview**
  - To compensate for a possible low answer rate

In chapter. 7.5 we will also investigate how feedback from customers being exposed to responsible gaming tools will show variation in relation with important sport events and positive/negative feedback.

The collected data will be basis for the initial part of the research question where we look at the situation related to the use of TET and PET techniques in European lotteries. The last part of the research question will be answered by doing closer examination and analyses of observations and collected data.

6.1 Questionnaires

Data collected by questionnaires will be collected by using a PDF document created in Adobe Forms sent by mail to individual recipients in European lotteries. This will ensure that answers could be collected by using check lists and scroll bars etc. effectively preventing phrasing errors and misunderstandings creating a homo genus data material. A online questionnaire tool could be used, but since the questionnaire most likely will be evaluated an handled by several persons at each company over time, a PDF document is chosen.

The recipients in each lottery were data protection officers and other persons working close to collection and use of personal data in each lottery. Many of them are members of international WLA[44] working groups and participants in security seminars hosted by WLA and other international security organisations like ISACA[45] etc. As a participant in different working groups and seminars I have met several of them face to face on several occasions. This would make it likely that they would be able to identify the origin of the survey and hopefully be wanting to participate in the study. Contact details will be collected from open

sources like company home pages, participation lists from seminars, public available publications etc.

A total number of 25 recipients is identified in lotteries across Europe.

The questions in the survey will focus on basic fundamental rights for individual data objects(customers) and data collectors/processor as stated in GDPR. GDPR should be familiar for all operators of lotteries making it easy to answer theses questions.

By collecting data pr. mail certain issues related to data protection will be raised. The answers could be related to individual persons with mail address etc. meaning that the data used in the study should be collected and processed according to GDPR and fundamental principles of data protection. Both technical features as mail address and even IP address is recognized as personal identifiable data. To ensure that the study complies with this principles and lawfulness the following measures is implemented:

- **DATA MINIMIZATION** - Only a absolute minimum of personal data to answer the research question is collected. This study will handle personal data identified as contact details(name. e-mail and the individual answers from those who choose to participate)
- **LAWFULNESS** - A written consent from the recipients is collected at the start of the survey. The participants could withdraw from the survey at any time by contacting a named contact person, collected data will then be deleted
- **INFORMATION** - Further information about the study and/or processing of data could be given by me as a named contact person with contact details in the received questionnaire.
- **DENATIONALIZATION/DELETION OF DATA** - Collected data will be deleted/DEPERSONALIZED at the end of the study and will not be used for other purposes or means

A comprehensive text with the descriptions of the study will follow each individual invitation, and the participants will also be invited to receive a version of the final study

To avoid ambiguous or misleading information a prestudy involving a handful of recipients will be conducted. After possible correction and clarifications is done the survey is distributed to all participants.

The study has also been approved by the Norwegian Centre for Research Data(NSD) on October 30. 2010. See chap. 12 for further details

6.2 Manual observations

To increase the individual value of the study, homepages for lotteries not answering the study will be reviewed manually. This will involve inspection of important documents/declaration like data protection policy/customer contracst and cookie policies to answer the same questions as in the received questionnaire.

I will be of specific interest to reveal if some web sites might be missing this information or if policies/declarations is misplaced and/or hard to locate.

6.3 Automated inspection of web sites

Both internal and external validity will be discussed in chap. 9 were collected data is analyzed and interpreted, At this stage I see no presence of specific needs or considerations related to data collection techniques or the questions in the survey. A question though could be the fact that some questions are detailed and might be difficult to answer for just one person. Most likely this will be no problem, but since collection of personal data is highly related to penalties for data breaches and company reputation it could also be tempting to present answers as more positive than the actual situation. This effect, known as the Hawthorne effect[46], is a typical example of reactivity where an observed person tends to behave in a way that he believe is expected to behave, or even express how things might should have bin(response bias). A typical example could be the use of cookie technology or information trackers. According to the planet 49[47] case a informed consent is needed from the data object before cookies is placed in the browser, but at the same time observations from web sites shows a highly variable practice and understanding of this judgement where third part cookies are set with limited or missing information. This could challenge the internal validity in the study, but according to Leedy et al.[46] this could be verified by introducing unobtrusive measures and do observations or collection of data unseen. Typical measures that could be introduced could be:

- Technical features like specific software to reveal the presence of third part cookies that intentionally/unintentionally could transfer PII to a third part.
- Manual inspection of data protection policies and cookie policies etc. to reveal discrepancy between observations, legal requirements and best practice/recommendations.

The possible presence of a discrepancy between observation and answers in the survey could be a result of the study itself, this will be further investigated in the following chapters where the existence of independent variables like cultural or historical differences ect. will investigated and discussed.

6.4 Focus group interview

To compensate for a possible low answer rate and lack of collected data focus group interview will be conducted to discuss the hypothesis from the study. According to Leedy et al.[46] interviews can provide a rich body of qualitative information, but it needs to be well prepared.

Members of the group will be resources and professionals in data protection, marketing and gambling addiction. The collected data from the interview will be compared with the observations in the study and hopefully confirm them, or at least give us further data for the analysis and discussions presented in chapter 7 and 9.

Both internal and external validity as discussed in chapter 9 should be improved since both quality and validity of the collected material would be better.

6.5 Internal and external validity

According to Leedy et al.[46] both internal and external validity of a study needs to be addressed to be able to draw meaningful and defensible conclusions from a study. The internal validity refers to which extent the researcher can make conclusions within the data material itself, while external validity refers to wether the results from the study is valid outside the situation of the study or not. Before the survey is initiated it will be natural to discuss both internal and external validity to reveal any problems related to techniques for data collection or research methodology.

There is number of arguments that could be used to describe the internal validity in the study is high, typical the facts like:

- All companies/participants has to comply with the same data protection laws(GDPR). This framework is implemented into national law, the understanding and details regarding the enforcement of the law is comprehensive described by EU authorities.
- Lotteries could be exposed to both cultural and regulatory differences, but they still sell the same lottery products making i likely that they are collecting the same type of personal data from their customers
- Data will be collected from a major part of operational lotteries in Europe making the data set highly representative for the business if the majority of the recipients choose to contribute

For external validity we see the same arguments as described for internal validity except the fact that there is no other other comparable lottery industries making replication in a different context challenging. The value of this argument would off course be limited since all processors/collectors of PII needs to be compliant with GDPR.

6.6 Results from the pre-study

In the prestudy an initial version of the survey was presented to three individual recipients for feedback. The feedback was given by mail/interviews where initial impressions and comments to design etc. were followed up by questions to give a deeper understanding of received concerns if needed. This will enhance the validity of the study as described by Leedy et al.[46] chap. 6. A short summary of received feedback was:

- Some questions tends to be to complicated to answer either yes or no. A typical example could be the presence of a dedicated policy for data suppliers where feedback indicates that this both could be handled as a part of the contract or use of a specific data processing agreement. To answer this problem the questions either needs more alternatives or clarification.
- To improve the quality of the answers boxes/fields for comments/additional feedback should be available for all questions. Available comment fields tends to be to small. This will improve the quality of the feedback
- Would it be natural to extend the survey to handle important lottery specific issues like the use of personal feedback as a responsible gaming tool. There are specific issues related to data protection that is of particular interest for lotteries

- How will you address the fact that lotteries also offer products not involving collection of personal data(Anonymous gambling like instant tickets or horse/sportsbetting)

As a result of this the following improvements were made:

- Comments fields were added to all questions, existing fields were made larger to make it possible to enter more texts and deeper descriptions.
- Some questions where rewritten to make them easier to understand
- Questions related to responsible gaming have been given a bigger part of the survey including theoretical text and definition of research question together with additional questions in the survey

The final version of the study were presented with the following subjects:

- Legal basis
- Access to customer data
- Responsible gaming tools
- Data protection policy
- Use of cookies.

7 Presentation of the study

The questionnaire was presented to 22 individual European Lotteries as a online survey at Nov. 10 2021 with two consecutive reminders in the following two weeks. A copy of the questionnaire is presented in chap 12(Appendix). The questionnaire is the initial part of the research question presented in chap. 5 where we collect data for further examination and analysis. As a final result I received 9 individual answers. The participants is presented in figure 3:

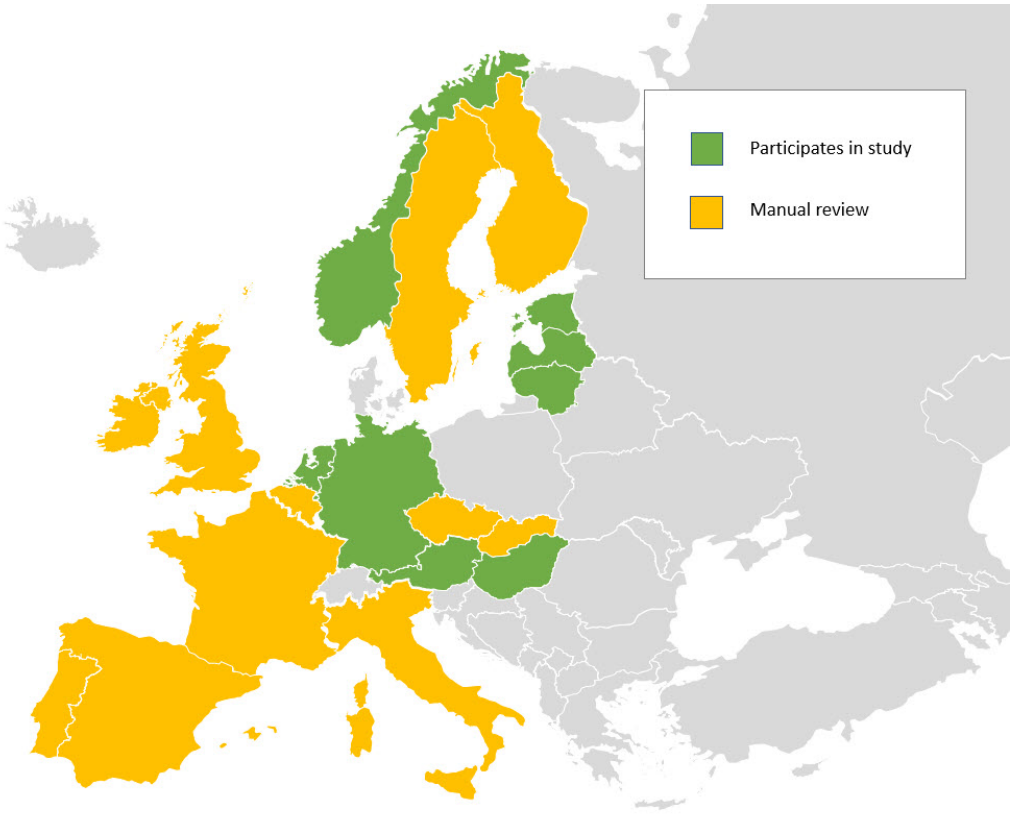


Figure 3: Participants in the study

The answer rate was slightly disappointing, but at the same time an representative answer rate in online questionnaires as shown by Vernet et al.[26]. A answer rate of 38 percent is according to this study low, but not abnormally low.

The following subjects where investigated manually, and the collected material will be used in the study:

- **LEGAL BASIS** - Description of legal basis in data protection policy etc.

- **DATA PROTECTION POLICY** - The presence of a data protection policy at company home pages with details about collected personal data
- **THE PRESENCE OF A DATA PROTECTION OFFICER** - The description of data protection officer at home pages/data protection policy together with contact details
- **USE OF COOKIES** - The presence of a cookie policy and cookie pop up bar etc.
- **COMPANY CERTIFICATIONS** - Documentation of company certifications at home pages

The collected materials will be presented as diagrams where participants 1-9 will be the companies answering the survey and 10-22 will be collected manually. feedback.

7.1 Legal basis

GDPR art- 6 states possible legal basis for handling of PII. Since gambling and participation in lotteries will involve establishment of a customer relation at some stage the following basis will be possible:

- **Customer contract**
  - Perhaps the most relevant basis involving acceptance of a customer contract with comprehensive description of terms and collection of PII.
- **Customer consent**
  - A specific consent for handling specific data types. Could be difficult to handle since any changes in collection of PII could involve collection of an updated consent from all customers. Some data like additional contact information could be collected with basis in consent since this kind of data is additional PII beyond the minimum data required for customer registration.
- **National law**
  - A general basis for handling of personal data. Needs to be documented and completed with additional data protection polices with required information to customers as describe in GDPR chap. 3. This legal basis could be recommended for monopolists giving a well defined role as a national regulator of lotteries and gambling activities.

17 out of 21 states that customer contract is the legal basis for collection of personal data while two totally relies on customer consent and one relies on national law. For one company neither data protection policy or any other information about data protection could be found at company home pages. One company states that both customer contract, customer consent and national law is legal basis, the last due to certain obligations made through the EU money laundry directive[48] from 2018

21 of of 22 companies has presented a customer contract or equal information about terms for disclosure of personal data at home page as presented in in figure 4:

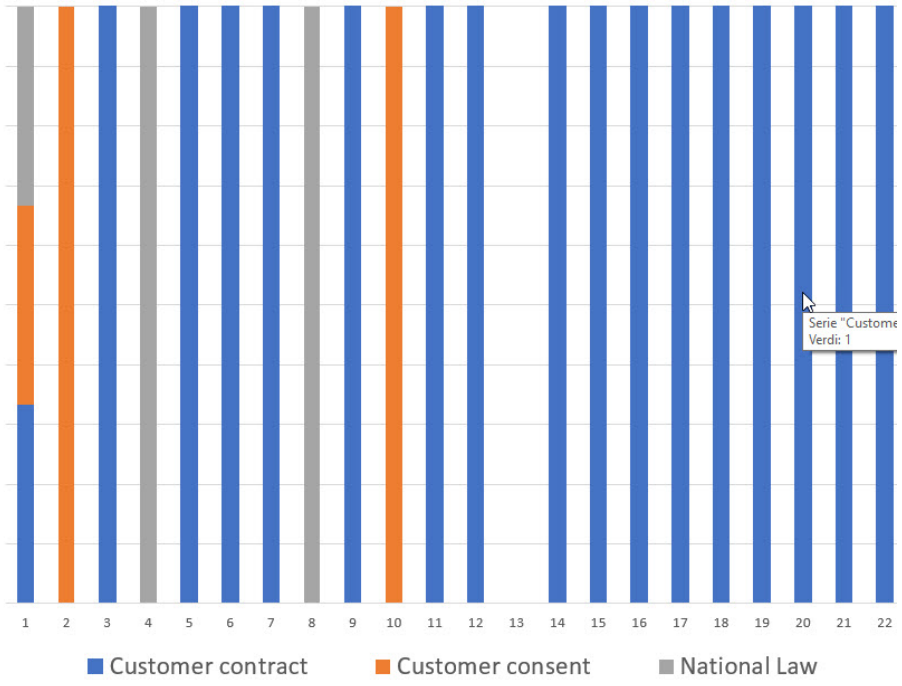


Figure 4: Legal basis for data collection presented in data protection policy

7.2 Collected personal data

Figure 5 documents the different types of personal data collected.

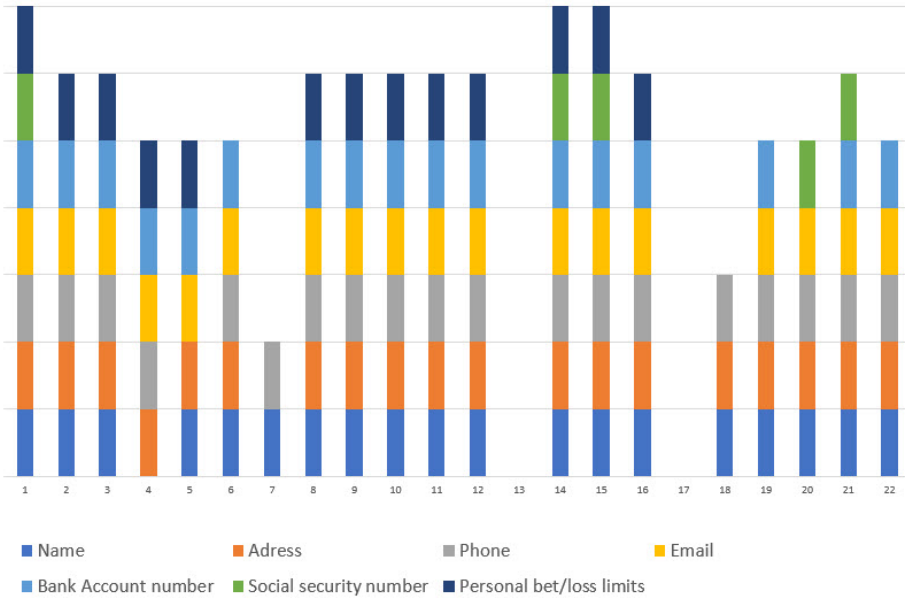


Figure 5: Personal data collected at registration

Considering that all companies offers registered gambling it is no surprise that personal data like name etc. is collected for this purpose. A small difference/variation seems to be collection of personal bet/loss limits and social security number. By those who answered the survey the majority states that this kind of information is collected, but by investigating the data protection policies for the remaining it is quite difficult to reveal whether this is done or not. Even though some of the polices are quite comprehensive and detailed this is not mentioned in detail. For two lotteries challenges related to language and access to relevant information made it impossible to make conclusion about collected data.

Other data collected are typical gender, and optional phone numbers. Only on single company informs that player picture and copy of player id is collected even though this is mandatory for physical registration of player details if the player chooses to register at retailer.(Ref. EU money laundry directive)[48]

There is a connection between fig. 4 and fig. 5 since using either customer contract, consent and/or national law will require some collection of PII at some stage to identify the customer.

7.3 Access to customer data

Of the 9 answers, only one company states that they not offer customer access to personal data online. Regarding what kind of data is available we see some differences in figure 6.

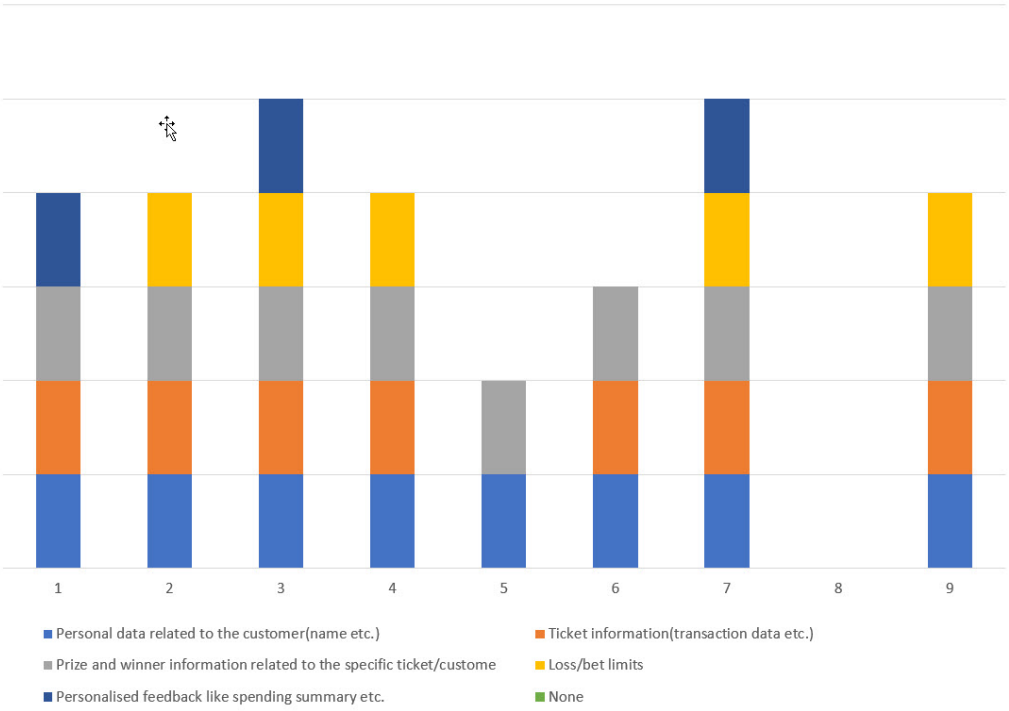


Figure 6: Access to personal data

6 out of 9 offers the possibility to correct errors in personal data while no one offers the possi-

bility to cancel tickets online. This could then only be done by making a request to customers service, and then only for tickets either sold/purchased by a mistake or ticket not paid by customer.

7.4 Responsible gaming tools

Behavioural tracking or use of player tracking/monitoring to prevent gambling problems is a relative new trend in the lottery business. It is strongly connected to online gambling since this kind of activity requires that the customer opens a personal customer account etc. giving personal data to the lottery as a part of a player identification process. Online gambling could be offered via internet or online lottery retailer terminals(LRT) at a lottery sales point.
The majority of gambling in Europe though is still anonymous making it difficult to collect personal data about the customer. As mentioned in chapter 3.6 responsible gaming tools could be self diagnostic tools, self exclusion or warning messages. 5 out of 9 companies states that this is in place while one is planning to introduce such tools in the close future. Only 3 makes the result of the tests available for later use by the customers.

Self exclusion is a widely used responsible gaming tool, and as seen in figure 7 the answers indicates that that 8 out of 9 has this tool in place. The last company informs that this will be in place within short time

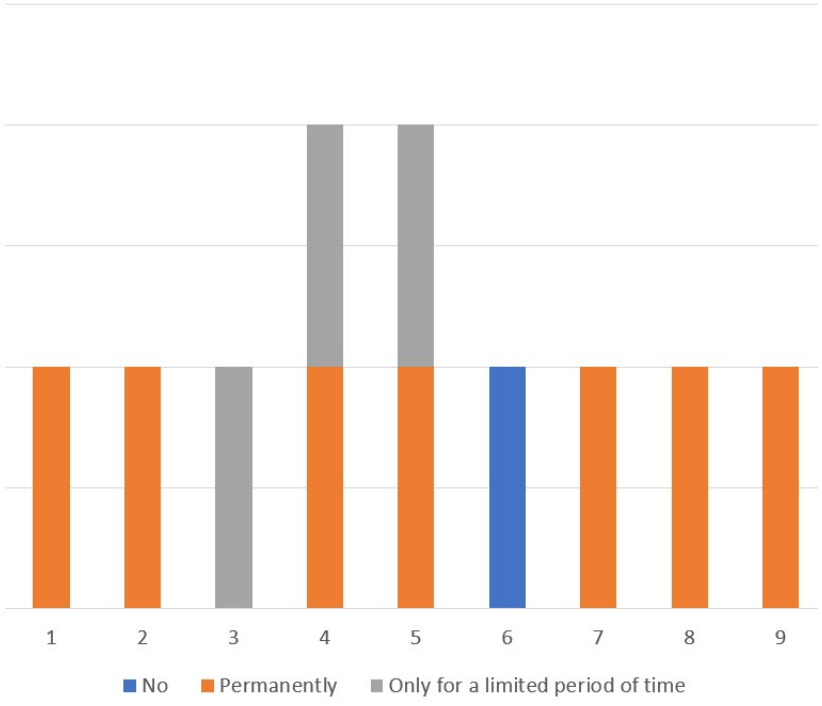


Figure 7: Self exclusion

Regarding warning messages only 3 out of 9 states that this is in place for different values

like time, and money spent etc. These kind of messages are typically used for online casino/roulette games where the player might be playing both continuously and repeating on the same kind of kind games. Several studies like Trivedi Teichert[49] and Auer and Griffits[50] shows that these kind of online games are highly addictive and more problematic than typical traditional Casino games.

There should be a correspondence between fig. 6 and fig. 7, but as we can see even though this kind of PII is collected the customer not necessarily have access to the data

7.5 Data protection policy

All 9 companies answering the survey states that a data protection policy is in place. A manual inspection of the remaining 13 lotteries reveals that this also is the situation for 12 of them. For the last company(no. 13) no traces or references to a data protection policy could be found, references to a cookie policy could though be found.

Chapter 2 in the GDPR gives detailed information about the principles of the framework for a data protection policy. A practical approach to create a data protection policy would be to reflected the details in these articles and describe how the company as a data controller relates to the requirements.

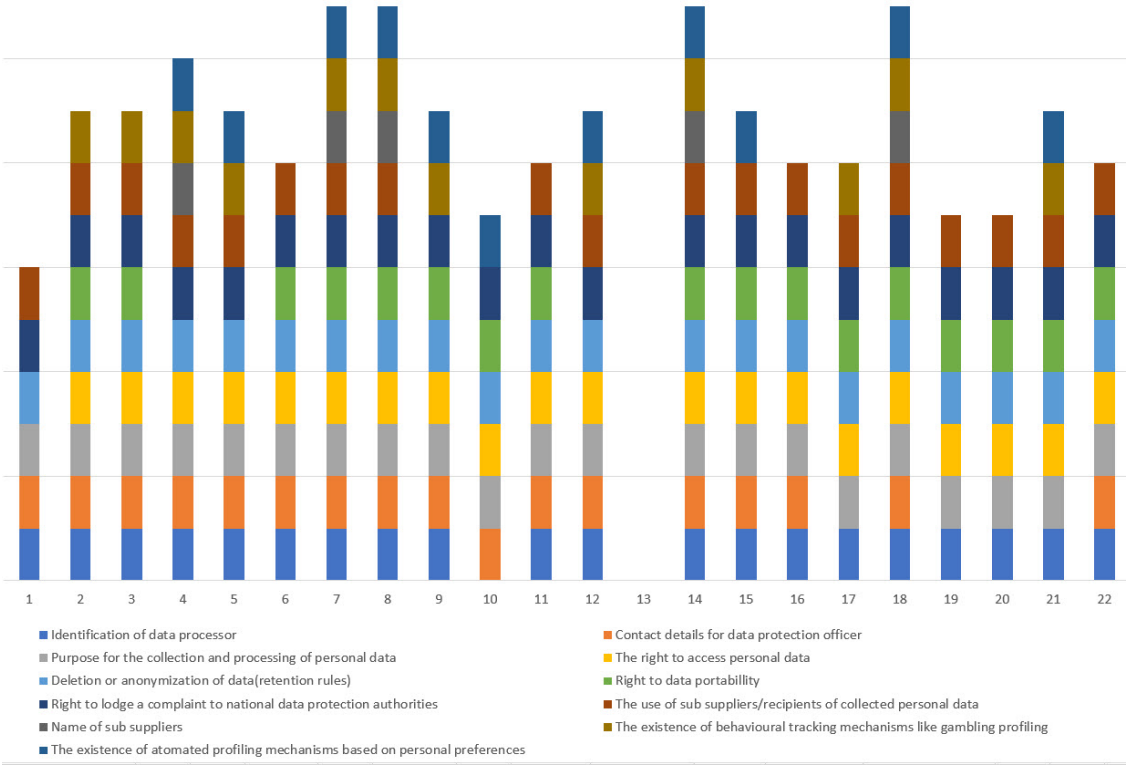


Figure 8: Data protection policy - Information

As presented in fig.8, there are some minor issues related to specific GDPR requirements like

identification of data processor, data protection officer etc.

17. out of 22 companies describes the presence and contact details for a data protection officer, but the findings and observations are to scattered to be able to suggest that there is a pattern or trend except that the level of details seems to be a bit low. Some differences can be seen for name of sub suppliers where only 5 out of 22 presents this kind of information. For behavioural tracking mechanisms 11 companies informs that this is in place for personalization based on personal preferences while 12 states that is is used for gambling profiling (Responsible gaming). The first number is interesting since this quite clearly documents that at least three companies uses this kind of tools without informing the customers(ref chap.6.8 where 3. part cookies were found at 14 web sites). This not according to the requirements in GDPR and could result in fines from national data protection authorities as described in chap. 2

For the 9 remaining companies we are missing information about the use/presence of these kind of tools since the survey not was answered or description not could be found in company data protection policy a.o.

8 out of 9 companies stated that they had company specific policies or guidelines regarding sub suppliers and processes and use of personal data in place. 7 out of 9 states that at company specific data processing agreement exists.

7.6 Anonymous disclosure of data

According to the EU directive on the protection of persons who report breaches of Union law[51], persons who warns about potential illegal activities(Whistle blowers) has fundamental rights to protection. According to art. 16, identity of the reporting person should not be disclosed to anyone beyond the authorised staff. In practical terms this means that a channel for anonymous disclosure of such data should be established. As seen in figure 9, 7 out of 9 companies who answered the survey states that this is in place. By manually inspecting homepages for the remaining companies none of them had this kind of functionality or description of how anonymous disclosure of data should be done.

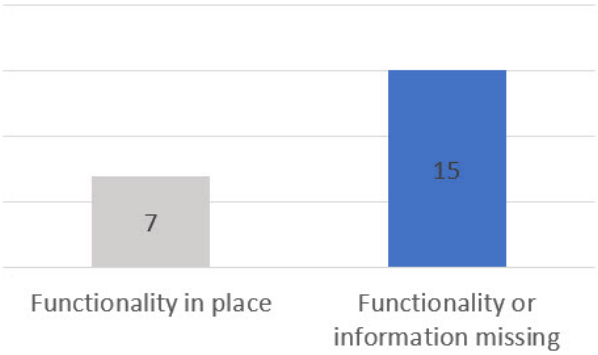


Figure 9: Anonymous disclosure of personal data

The lotteries that actually claimed to have this functionality in place and answering positive

to this question in the survey were also inspected manually. At least several of them presented no such functionality despite giving a positive answer. It could be that this was only available for customer logged inn with username as registered players, but it could also indicate that the answers to this question were misleading or even wrong. Further investigation of this problem turned out to be difficult since customer registration requires at national citizenship and ID mechanisms to be able to establish a customer relation.

7.7 Information about data breaches

All 9 companies that participated in the survey answered that they would notify the involved customers in addition to national data protection authorities in case of a unintended disclosure of personal data.

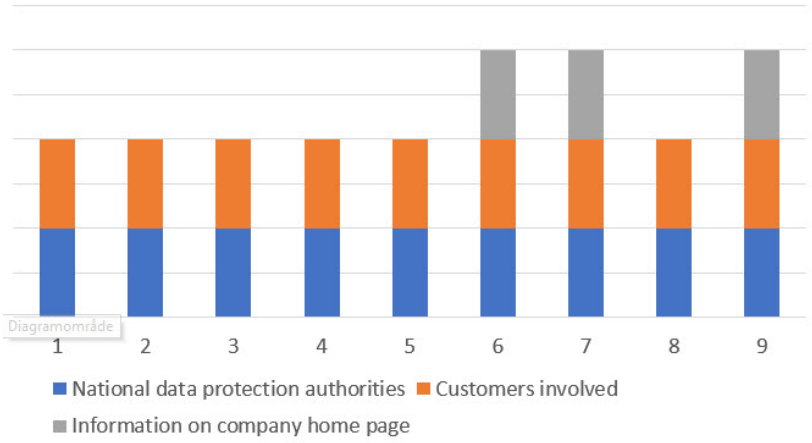


Figure 10: Data breach information

As seen in figure 10, 3 companies stated that they also would release information about the breach on their home pages

7.8 Use of cookies

Cookies are basically small programs or program interfaces that allows storage of information related to visits to different web pages. This information is retrievable for either the browser/user of the browser or by the owner of a specific website. Some cookies commonly referred to as tracking cookies collect information about customer behavior across web sites typically to present marketing data such as personalized advertisements(re-targeting)

According to the Eu ePrivacy directive[13] and the later understanding of GDPR and use of cookies and tracking tools, a informed consent is needed from the user before a cookie could be placed in a browser. An informed consent is an expression from health services where the intention is to get permission from a patient before a specific medical treatment is initiated. A clear appreciation and understanding of the facts, implications, and consequences of an action is essential. If we transfer this to the use of cookies, this would typically be done by informing user through a cookie policy/declaration and collected consents from user. By inspecting company pages manually only 2 of 21 companies was missing a specific cookie

declaration at their home pages. 7 of 22 homepages were missing a consent management platform for cookies displayed to new visitors at company home pages

Cookies could basically be categorized as:

- **Necessary** for web site functionality
- **Functional** cookies used to remember personal preferences and settings
- **Statistical** purposes
- **Marketing purposes** like display of relevant adds across websites etc.

There is some variation regarding the categorizing of cookies, but all inspected policies seems to relate to the suggested categories described in the text. Some companies though are missing either necessary or functional cookies and seems to present them as one group.

By combining the answers from 9 participating lotteries and manual inspection of data protection/cookie polices for the remaining lotteries the following summary showing the existence or description of used cookies could be produced as seen in figure 11.

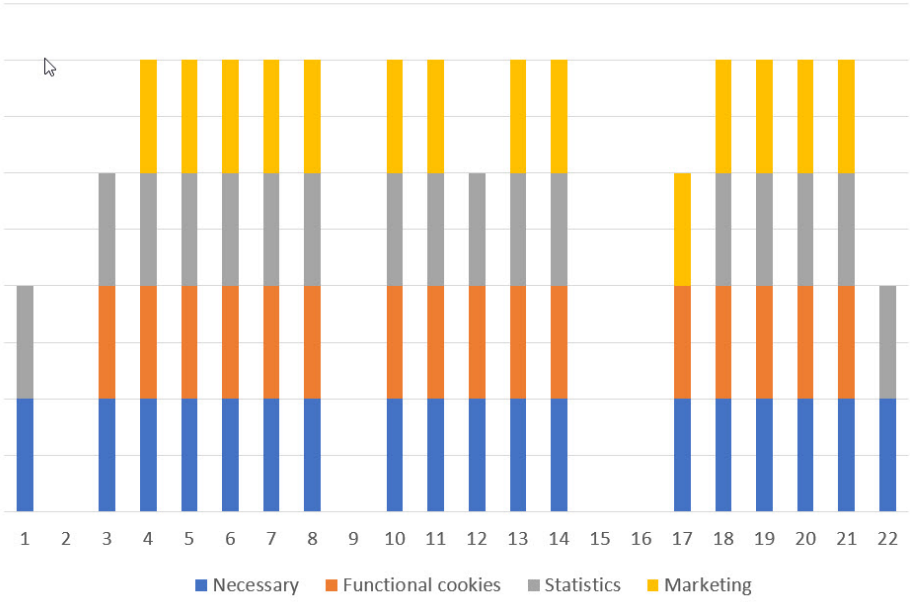


Figure 11: Cookie information

Cookies could be disabled by deletion in browser or by offering functionality at web pages. 8 out of 21 offered this last functionality while the remaining 13 describes the possibility to delete cookies int their cookie policy/declaration. The quality of this documentation could be rated from a high level with detailed information to almost no description at all.

3 out of 9 participating lotteries states that they collect consents for personalization.(most likely involving the use of of 3. part/marketing cookies) Another 4 has this information in their cookie/data protection policy, but functionality for collection of consents cannot be

found at home pages, most likely because this is only available for logged on customers. 14 lotteries neither collects consents for cookies or informs about the use of cookies in their data protection/cookie policies. It seems like at least some companies is using cookies without informing customer/visitors to home page(ref. fig.11). This 'cookie bias' will be further investigated in chapter 7.

7.9 Export of customer data

On the question whether the company offered the possibility for the customer to request a copy of his/hers data or not, 2 companies answered this question positively while 7 others only offered this functionality on request as presented in figure 12.

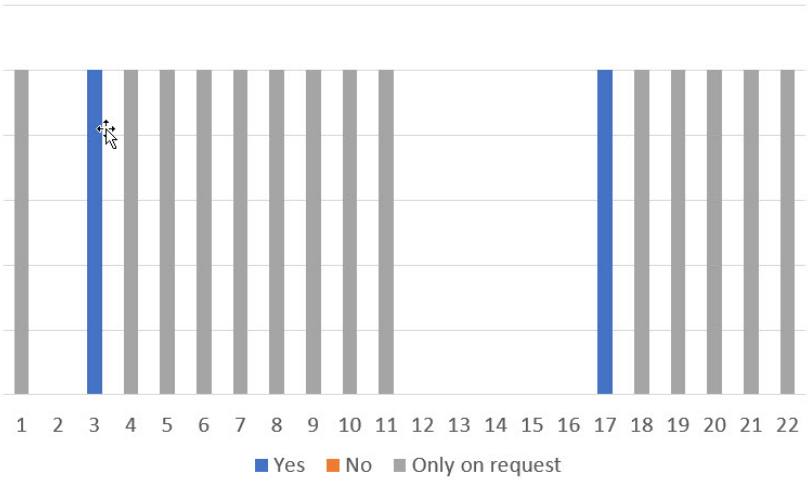


Figure 12: Export of personal data

For the 14 companies this was described in data protection policies etc., but again with great variation in level of details and accessibility since some data policies tend to be long text documents not specifically easy to read or understand. 6 companies either failed to answer the survey or had no description in data protection policies etc. making it hard to read and understand

7.10 Company certifications

All 22 companies were certified to the lottery specific WLA SCS security control standard. This certification is described in chapter 2. WLA offers a updated list of all certified companies at their home pages, making it easy to verify that specific lotteries is certified or not. Regarding ISO 27001, this is a bit more difficult to verify since this certification is done and maintained by national/local certification bodies. By inspecting company home pages and look for the ISO 27001 logo or similar information, the following the following summary could be presented as seen in figure 13. The most important finding related to certifications seems to be that the WLA or ISO 27001 logo not is used at several company home pages even though the company is certified to one or both of the standards.

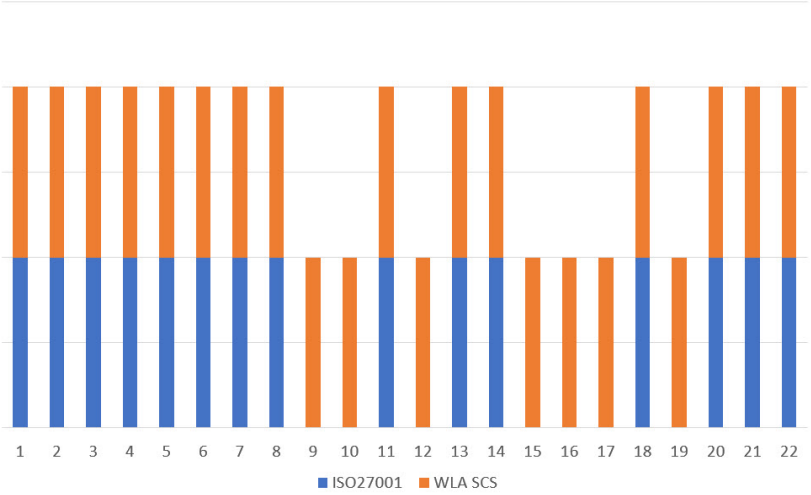


Figure 13: Company certifications

7.11 Result from the focus group interview

As all ready presented in chapter 6, a focus group interview could be conducted to improve the quality of the collected material in the study. As an complementary action this was done after a low number of questionnaires were returned in the survey.. The group consisted of 5 members and me as moderator. In addition to the presented topics a series of questions and follow up questions were prepared, all related to the research question, but not presented to the group members in advance. As a result of the spread of the Covid-19 virus the interview was conducted online as a Teams meeting, but since this tool was well known by the members this was be no limitation. The following subjects were discussed during the meeting:

- **Could data protection be a market advantage and provide customer trust.**
  - Is there a connection between customer trust and data protection?
- **How does lotteries provide transparency to customer in relation with collection and use of personal data**
  - Data protection policy and customer contract etc.
  - Responsible gaming
- **How can lotteries improve transparency**
  - New technology like AI and machine learning
  - Blockchain technology
- **Differences related to data protect**ion in Europe
  - Geographical differences
  - Monopolist VS shared market
- **Is there a connection between data protection and certifications like ISO/WLA**
  - Is the ISO 27001/WLA certification and andvantage.
  - Other certifications and use of ISO/WLA logo at company sites

7.11.1 Summary of the focus group interview

- **Data protection could be an business advantage**

  All member of the group agreed that data protection could be a business advantages if presented to the customer properly, but at the same time the effect could easily be devastating if misuse or even illegal use of personal data is revealed. Monopolist lotteries in general also has a high level of trust among customers and population, typical reflecting a low number of questions and feedback related to use of personal data and request for access to personal data in general. Monopolists is more regulated and controlled than illegal/unregulated operators offering their products in the same market. Northern Europe seems to be more regulated than the Southern parts even GDPR applies to all EU/EEC countries

- **Handling of PII could be improved**

  Lotteries are in no way better more transparent than other businesses, but the potential to improve this is very much present. The industry in general could learn from Google a.o. who presents a personalized message to the customer making it possible to adjust commercial messages, delete tracking data(at least to some extension) etc. Some data like high prize winners and gambling problems is highly confidential information that must be handled both safely and accurate in relation with transparency and accessibility.

- **Showing transparency towards the customers is challenging**

  Showing transparency and explaining the use of personal data to the customer is challenging since data privacy policies and cookie policies is hardly ever read by the customer, and if they are, only in relation with problems and complaints. This is quite typical since the origin of these policies traditionally is inside out providing compliance for the company and not outside in written for the customer for best possible understanding. We need to explain to the customer more clearly what we are doing and why, but again to much text and difficult language is not very user friendly.

- **The effect from cookies and user tracking could be limited**

  The use of cookies and tracking techniques for re-targeting and commercial purposes is connected to the market situation were lotteries operating in a market with other competitive lotteries typically have more focus on marketing and visibility than monopolists. Gambling and user tracking has a limited accuracy level and could possibly create no real values for the customer. Overexposing gambling could be perceived as irrelevant and both cynical and irresponsible. Personal messages and communication in general is closely related to the individual customer making it challenging to produce specific messages and information for individual customers. On the other side, service

information in relation with ongoing customer activities tend to be very positive as long as it helps the customer with problems and improves the customer experience in general. One of the best and most effective examples is typically customer accounting services where the customer can choose when and how to receive information about win/loss, stakes etc.

- **Personal data and responsible gaming activities is important**

  The use of personal data in responsible gaming activities has the ability to target customer individually, but at the same time we need to have a clear understanding of what we are trying to achieve and how. Improved knowledge about customer behaviour and available techniques is crucial for success and have a great potential for further improvement. A potential threat from AI and machine learning in relation with change of customer behaviour is that we might effectively address some groups and fail to communicate with other smaller groups. This must be taken into consideration and makes it likely that this kind of techniques will be used as a supplementary tools together with human interaction.

- **New methods for data collection raises ethical questions**

  At the end of the interview several of the group members expressed concerns about the ethical issues with data protection and use/misuse of personal data. New technologies and methods for data collection raises some serious questions about how fare we are willing to go and when we should stop. Ethics and laws seems to evolve slower than technical features and calls for closer definitions and frameworks for collection and use of personal data.

8 Analysis

Like already mentioned the answer rate of the survey ended up quite low. It is difficult to determine why this happened even though the participants in the survey were well known by me and were approached through a personal invitation. By investigation the map in figure 3 some details still could be revealed, and even some of the feedback from the participants could give a partial explanation as well

Among the 9 lotteries that answered the survey the majority with only one exception are national lotteries with exclusive rights to gambling operations in their country or geographical area. Two German lotteries participated, both monopolists in their provincial region. At the same time I also received comments from other lotteries explaining that some of the information asked for in the questionnaire were considered critical to their business operations, typically:

- Number of customers/employees
- The presence of tracking tools
- The use of responsible gaming tools
- Name of sub suppliers

Countries with a partly legalized lottery marked is typically found in the Southern part of Europe while Scandinavia/the Baltic and other countries in the Nordic hemisphere has a more strict and regulated market typical with one governmental operated lottery or limited number of operators.

Several answers did i.e not contain information about number of individual customers a.o. This could mean that some of the invited lotteries chose not participate in the survey because they not wanted to share any kind of information with other lotteries etc. This happened even though the invitation to the survey clearly stated that all data would be handled anonymously with no references to the individual participants.

I also needs to be mentioned that the some of the lotteries in the study offer anonymous gambling products with no registration of personal data in combination with registered gambling. The impact to this study and number of returned answers is hard to evaluate, but it could indicate cultural differences. Almost all lotteries in Europe offers these kinds of products, but again we see that the majority seems to be located in the Southern part of Europe where anonymous gambling is more common than in the Northern countries.

The observed differences is supported by other studies like O'Neill et al.[52] who found that response rate varied regionally. Highest response rate where found in countries from Northern Europe and lowest in Southern European countries. Schwartz [53] even found that response from public institutions was significantly higher than other groups. Both studies supports findings in this survey where national lotteries i Northern Europe seems to be more

willing to share information than other lotteries.

A low answer rate could question both internal and external validity. I believe though that the received answers is representative for at least some parts of Europe/type of companies and give a valid data material for further discussions, conclusions and recommendations.

8.1 Legal basis

Legal basis for handling of customer personal data is describe in GDPR art.6 as

1. The data subject has given consent to the processing
2. Necessary for the performance of a contract to which the data subject item
3. Necessary for compliance with a legal obligation to which the controller is subject
4. Necessary in order to protect the vital interests of the data subject or of another natural person
5. Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6. Necessary for the purposes of the legitimate interests pursued by the controller or by a third party

Customer contract is mainly used as legal basis for handling of personal data by European lotteries, but the survey itself says nothing about the quality of the contract. Required information at registration should be according to GDPR art.13, meaning that it basically should be identical to the data protection policy. As seen in fig.8 the observed data protection policies in the study were both incomplete and lack certain required details. A GDPR compliant contract is essential to be able to claim customer contract as legal basis and needs to be compliant with art. 13

National law could be and alternative since many of the participating lotteries operates as governmental monopolist. This could typically indicate that national laws exists to regulate gambling operations with specific reference to handling of personal data in the interest of a official authority(GDPR art. 6.2). GDPR is still valid, and customer/data object is required to have the same information as any other used legal basis. National law could also indicate that legal basis on other national laws could be present. The most important law to consider would be the EU Anti-money laundering directive that is implemented for all EU/EEA states. According to art. 30 in Norwegian national law(The Anti-Money Laundering Act)[54] obliged entities may process personal data to comply with this law. Information to customer/data object is still required as described in art. 14. Information that could be collected with reference to this law is a copy of valid ID and information about politically exposed person (PEP). This would be a person entrusted with a prominent public function as described by Wikipedia a.o.[55]

Consent as described in GDPR art. 1 is also used, but then to reflect that additional data is collected for a specific purpose like SMS messages, e-mail communication or even personalization based on personal preferences

The survey shows that different legal basis is in use, but there seems to some discrepancy between legal requirements in laws/regulations and information given in data protection

polices, customer contracts etc. To be a valid legal basis for handling of personal data this must be in place and calls for a closer examination to ensure a sufficient compliance level.

8.2 Collected personal data

Art. 5 in GDPR states that personal data shall be collected for a specific purpose and limited to what is necessary in relation to the purposes of the collection. The result of the survey as seen in fig. 5 leaves very little doubt that this actually is true. Collected data are limited to personal data like name, address etc., information obviously needed to both sell games/give a positive ID of the player and make a correct prize payout. Regarding personal bet/loss limits this seems to partly reflect the participants in the study as shown in fig.3. This is no surprise since these kind of limits refers to a personal customer account and customer registration/disclosure of personal data as. For anonymous gambling products this kind of limitations does not exist. The existence/collection of bet/loss limit is also a indication of the maturity level in the specific lotteries. This kind of responsible gaming tools is becoming more and more used as both national and international regulations aims to reduce the effect of gambling problems and only allow registered gambling.

Social security number reflects the user identification process where customer identification not necessarily involves the use of this PII. In Norway a customer could i.e. be unidentified through the use of BankID[56] or even payment services like VIPPS[57] making the use of social security number obsolete. Similar products or registration processes exists for other countries as well including one time password and/or two factor identification.

For customers that chooses to register physical at company retailer this will involve the use of a ID like drivers license or passport etc. The EU Anti Money Laundry Directive[48] (AML directive) requires the registration of a copy of official document which confirms their identity, residential address and date of birth.(Customer due diligence). This kind of information is not a part of the questionnaire, but the participating lotteries where asked for additional collected information. Only one company informed that they collected this kind of data. As already described data protection policies where inspected manually to reveal the existence of collected PII(Personal Identifiable Information), but references to the AML directive where either missing or briefly described as data related to obligations to applicable laws and regulations. Again we see a lack of detailed information related to collection of personal data where details are either missing or presented with a insufficient detail level.

It is a paradox though that the AML is applicable for all lotteries and/or financial institutions making it likely that companies offering anonymously gambling might be running their operations in violation with the AML requirements. This kind of operations could be anything from low prize instant ticket lotteries to high prize major national lotteries involving both possible money laundry and/or transfer of money to criminal activities.

Information about collected personal data will be a typical transparency enhancement technique(TET), but it will also involve transparency related to lawfulness and compliance with national and international laws and regulations. As a player, access to details about collected

data in combination with retention rules and possible transfer of data to public authorities would show that the lottery acts within a defined and described set of rules, and would be a typical characteristic related to trustworthiness (Chap. 4.3). Transparency related to lawfulness and compliancy would be a natural extension of this and assure that integrity towards handling of PII is both documented and published in public.

8.3 Access to customer data

Access to personal data is an important privacy enhancement tool(PET) showing transparency and correspondence between the customer impression of collected data and the actual data collected by the data controller. This is especially important for the gambling industry who need to show the numbers etc. you have played and the final result of the draw with a potential payout etc. This is also reflected in the answers where 8 out of 9 lotteries offers access to personal data and prize/winner information

There are some differences related to access to loss/bet limits and personalized feedback(spending summaries etc.). This is typical responsible gaming tools, and could indicate differences in the maturity level for the individual lotteries as described in the previous chapter.

No lottery is offering the possibility to cancel tickets which off course is a big difference from typical web shops where cancellation and return of products is an important service towards the customer. Considering the characteristics and nature of a lottery, cancellations and return of tickets is highly questionable. Experience show that this kind of functionality is closely related to illegal activities like attempts to change the odds by cancelling short time before cut off/match start and manipulation of bet/loss limits. It i also technical challenging to handle cancellations in relation to multi week/game wagers, syndicate(multiple ownership for tickets) and return of money. As a result of this most lotteries has strict regulation for cancellation, only allowing cancellation by request to customer service for erroneous purchases.

Correction of errors in personal data is a also an important PET tool giving the customer/-data object the possibility to maintain his/hers own personal data and increase correspondence/trust. Some personal data like social security number is not possible(or at lest should not be) possible to correct since this would make is possible to manipulate personal bet/loss limits and make tracking of activities related to money laundry impossible. The result also shows that the majority of the lotteries(6 out of 9) offers this kind of functionality. For those not having this in place it would make an great improvement to implement this functionality.

8.4 Export of personal data

Export of personal data is recognized as part of the fundamental user right of access to own personal data as described in art 15. Art. 20 even describers the fundamental right to data portability as having the right to receive the data in a structured, commonly used and machine-readable for possible transmission to another data controller. The difference between observed functionality and legal requirements is quite eminent(ref. fig. 12) since

only two lotteries offers this kind of functionality, and the rest either will offer it only on request or have no/limited information about data export on their web pages. Lack of export functionality is a little bit of a surprise since access to own data not only is a fundamental right, but also an important responsible gaming tool considering that collected/stored data will involve loss/bet information, important indications of a possible gambling problem. This subject will be discussed in chapter 8.5

Regarding information about data export most lotteries briefly describes the details lacking important details like possible data format, what kind of data will be exported etc. As a summary there seems to be a significant difference between available functionality and requirements in GDPR.

8.5 Responsible gaming tools

Several participants in the study refers to the use of responsible gaming tools as described in chap. 4.7. We have seen that a major part of the lotteries collect data as personal loss/bet/exclusion limits, grants customer access to customer data and transaction data and finally offer online tests to reveal problems related to gambling. In short they could be summarized in two groups:

- **DATA COLLECTED FROM THE CUSTOMER EITHER MANDATORY OR VOLUNTARILY:** This would be loss/bet limits ore even self exclusion from gambling. Different limits could also be present as a part of the general rules for gambling or even specifically set for individual games. According to Blaszinsky et.al[58] the advantages of these kind of tools is the ability to reach many gamblers at different levels of risk, but only having a low to moderately high effect.
- **TOOLS FOR SELF TESTING AND/OR CUSTOMER PROFILING:** Several software tools like Neccton[35] and Playscan[36] offer customer segmentation according to customer behaviour, personalized/targeted feedback and behavioural insight reports etc.

According to Auer and Griffits[50] targeted personalized information can be an effective tool for online gambling companies to reduce gambling expenditure. Other experimental researches like Monaghan and Blaszinsky[59] even found that the content of the message is important. Seniors seems to prefere messages concerning gaming limits while younger groups tend to more positive to messages concerning their individual play and losses. Both studies also document's that general warnings seems to be ineffective while personalized feedback is more effective when it comes to changing or modifying players thought or behaviour.

Playscan is used by Norsk Tipping since 2017 as a responsible gaming tool. By tracking bet/loss, game type spent time etc. it will provide a risk profile indicating whether the specific player is in risk of developing av gambling problem or not. Each week i.e 1.6 millions player transactions is analyzed, and the result of the analysis would be a customer 'playscan profile'(Red, yellow or green) that will trigger specific actions towards the different groups. Green players would be able to continue as normal while those who are categorized as red players could receive personalized feedback, be blocked for marketing marketing measures or have to do a self test to reveal gambling problems etc. A total of 850 individual messages is available for personalized feedback to individual players.

As a part of the self test, customers are given the opportunity to give their feedback to the use of the tool. A total of 1068 individual messages where collected from 2018 to 2020 by Norsk Tipping. By examining the collected data time, number of feedback and types of feedback could be investigated closer.
Basically feedback could be divided into four groups:

- Clearly positive
- Clearly negative
- Explaining, trying to explain the result of the test
- Uncategorized

If we combine the collected data with important sport events etc. as seen in figure 14 we see typical peek levels at 2018 Football World Cup and low levels in holidays

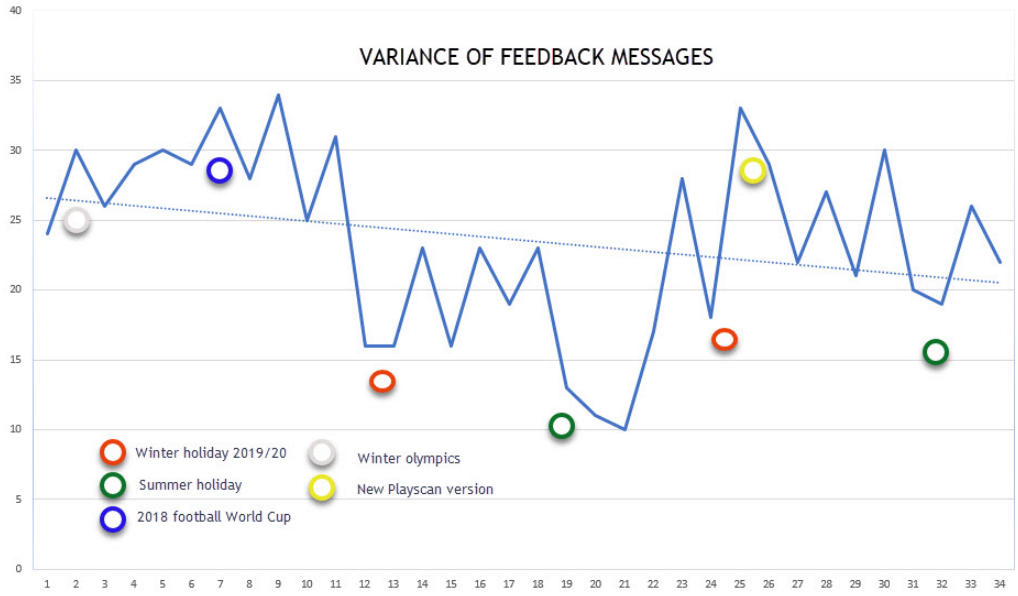


Figure 14: Feedback variance

The tendency seems to be that number of feedback messages is dropping over time with peak levels relate to:

- Important sports event like 2018 Football world cup and winter Olympics that increases gambling(Typical sports betting).
- System upgrades that introduces new RG features that triggers more feedback
- Periods with lack of sports event that seems to reduce number of feedback messages.

If we place positive and negative feedback in the same figure as seen in figure 15 we can see that negative feedback seems to come before positive feedback with almost identical numbers in each group

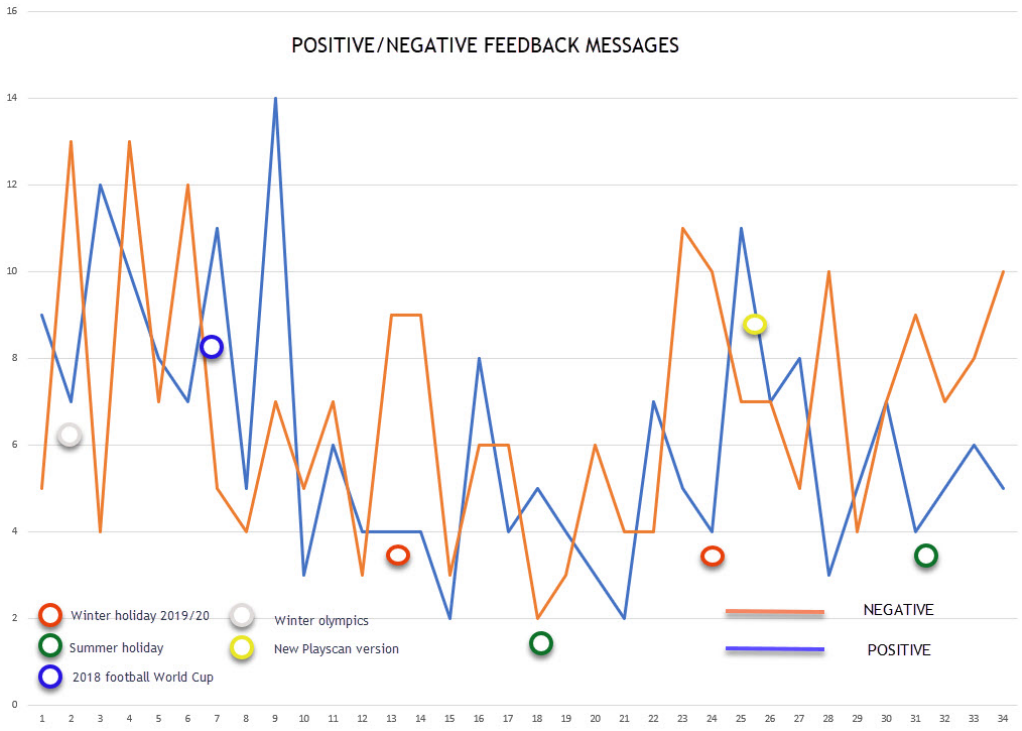


Figure 15: Positive and negative feedback

The reason could be that negative feedback seems to be coming from high involved players reaching loss/bet limits in relation with important sports events. These players will also be classified as high risk players according to the Playscan classification model. A well know fact is also that those who have a negative impression also are those who most likely will give their feedback. If we combine positive feedback message with those that try to explain the result of the test we see an almost identical and overlapping pattern. By examining the different feedback messages, many of them are related to how players experience Playscan involving descriptions like 'RG tools is double standards since the main purpose of gambling is revenue' and 'illegal tracking' etc. Other players tend to be more reflecting telling that RG tools makes them feel safe or trying to explain the result of the test.

This observation is also confirmed by Svenska Spel[60] who completed in depth interviews with 10 customer loosing more than 50.000 SEK in 2020. These customers had to take a self test to be able to continue playing. Many of them clearly stated that they where offended by this decision and felt that the lottery where tracking them illegally. These kind of expressions also reflected that they had no, or at least were lacking understanding of why they had to take the test and what the result of the test would be. It became quite clear that both transparency and and the way information about the test where given were crucial. If information were given in a clear and explaining language with no condemning undertone it was more likely that the use of RG tools were considered being positive. Several studies like Griffiths

and Auer[61] and Forstrom et al.[50] support these findings and indicates the need to use qualitative and personalized feedback to be successful. Both studies documents that targeted messaging can be an effective tool to reduce gambling. Forstrom et al.[61] explores a user paradox in their study showing that repeated usage of voluntarily RG tools is low partly as a result of lack of feedback to the users. Gamblers seemed to have a positive attitude as long as the given information is easy to read and are well written, but the given information must be both precise and given at the correct time.

8.6 Data protection policy

A well written data protection policy is a key element when it comes to showing the organisations commitment related to data protection and GDPR compliance level. It should give an overall insight in how the different parts is implemented and be written in a clear and understandable language making it possible for both customer and employees to understand the content and meaning. A data protection policy is typically presented as an active link on company home page with references to further details like contact points, technical features etc.

As presented in chap. 3.7 a comprehensive data protection policy will be typical TET (Transparency enhancement tool) showing the data object how the data processor relates to both legal requirements, data protection principles and user rights. A data protection policy will also be the natural place to start if National Data Protection authorities would require proof of compliance level from a data processor or data controller.

There is no specific GDPR requirement related to the establishment of a data Protection Policy, but art. 24 states that the organization should be able to demonstrate that the handling of PII is done according to the requirements in the regulative. Furthermore, important issues related to rights and interests of the data object is stated in art. 5 and 13, all reflected in fig.8. It is a paradox though to see that even though the required content of a data protection policy is clearly described and documented, so many companies in this survey fails to include important parts. As already mentioned i chap. 8.6 the observations are scattered, but clearly they indicate a lack of quality in the reviewed policies. A lack of quality in this context indicates that the policies fails to meet the expectations in GDPR typically by:

- Missing important required information like contact information and existence of tracking mechanisms
- Using a difficult language making them difficult to both read and understand
- Being hard to find

As presented in chap. 6.5 a data protection policy was found for all companies with on exception, but the quality of the policies varies greatly. A partial explanation could off course be personal perceptions of what a Data Protection policy should look like, but still it cannot explain why important details like contact information, existence of tracking mechanisms etc. is missing. A poorly designed or written Data Protection policy is no enhancement for transparency. Considering that it also could be both hard to find and even partly inaccessible as observed for some web pages it would be the other way around. By not exposing publicly in a clear and understandable language the purpose and details of the collection of PII it

could easily leave a negative impression of the intentions and understanding of the collection of PII. As discussed in chapter 4 this could lead to increased privacy concerns and reduced trustworthiness

8.7 Anonymous disclosure of data

Just as the right to be informed about the collection and use of PII etc. it could be argued that the right to anonymity is a equal fundamental right related to data protection. The EU directive on the protection of persons who report breaches of Union law[51] has not yet been introduce to Norwegian legislation, but almost similar right to whistle blower protection could be found in the Working Environment Act(Arbeidsmiljøloven)[62]. When legal basis for anonymously disclosure of data is identified as a legal requirement is is a paradox that only 7 lotteries actually offers this functionality(Ref. figure 9.) on their web pages. It could be that this functionality is described as a part of other documentation than company data protection policy etc. and not found/observed in the study, but still it is a significant number of companies not offering anonymously disclosure of data. Considering that lotteries and gambling is strongly connected to money laundry[63] it is a bit surprising that so many choose not to offer this functionality.

8.8 Information about data breaches

According to GDPR requirements data breaches should be reported to national data protection authorities and those affected by the breach. 3 out of 9 companies answering the survey informed that they also would give the similar kind of information to customers at their company home pages. This low number is understandable since data breaches could involve investigation, fines and possible damage to company reputation. Exposing weaknesses in infrastructure and technology would leave an impression of lack of control and knowledge etc., definitely no boost to company trustworthiness. On the other hand, if the company could show a high level of data protection and also had sufficient resources and guidelines in place, it could be argued that correct handling of data breaches in fact would be beneficial for company trust.

As described in chapter 4.4 the ability to handle a situation within a set of acceptable rules is crucial to show integrity. Correct handling of data breaches including full transparency towards customers would show the ability to act correctly leaving an impression of professionalism and high preparedness level. If the company fails to handle the breach this way it could easily give the impression of unpreparedness and lack of both skills and knowledge.

8.9 Cookies and tracking tools

As described in chapter 7.8 the result of the survey indicates the presence of a 'cookie bias' where the participating lotteries either fails to declare their use of cookies or provide insufficient or even misleading information in cookie policies etc. This refers both to general information about cookies and collection of consents which according to the EU cookies directive[13] is needed before any cookies are placed in a browser. The fundamental principles of the directive is to:

1. Provide clear and precise information about the cookies (including strictly necessary ones) and their purpose when users visit a website.
2. Get prior consent from users to store the cookies on their device
3. Make available an option for users to deny consent to use the cookies.
4. Make the means of providing cookie information, opt-out option, and requesting consent as user-friendly as possible.
5. Allow access to website content that may not use the cookie denied by the users

To actually inspect the different web pages and verify that they either are compliant with these principles or even verify that the information supplied through the survey actually is correct two techniques is used:

1. **Manual inspection of cookie policies and consent management platforms** - This could be challenging since this kind of documentation not necessarily is easily accessible and could be a part of a larger document with more or less general information about information security etc. in general. It could also be problems related to language and translation
2. **A comprehensive list of used/installed cookies** - Every company/web page i the survey places some kind of cookies in browser. This could be inspected/seen in the browser history itself, but to get a fully picture of installed cookies, cookie preferences and data communication a specific tool for this purpose is needed. The examples in this text is produced by 'Cookie Information - Privacy management platform'[64]. Other tools exists in the market, but after some testing this specific tool turned out offer the necessary technical functionality and report options.The supplier also offered unlimited access to their functionality for students as a part of their corporate social responsibility policy together with technical and professional guidance. Both become very handy since understanding the use of specific cookies and test results is challenging. Details about specific cookies and data collection tends to be both hard to find and lacking details.

Initially sites who either claimed that they not used cookies or had no policy regarding use of cookies present at their home pages were inspected. For these sites only 1. part cookies could be documented, most likely used to improve functionality by storing username/password locally etc. A special observations though was that one company who answered that no cookies were in use actually placed several and also offered the user to give his consent to the use of different types of cookies together with a cookie policy. This kind of observations was also done for other inspected web pages were a bias between information reported in the study and/or in cookie policies/information could be observed. The most typical example would be the existence of 3. part tracking cookies even though this was not reported in the study or any information could be found at the different web pages. Another example would be the

quality and accessibility of needed information. A typical example could be seen in fig. 16

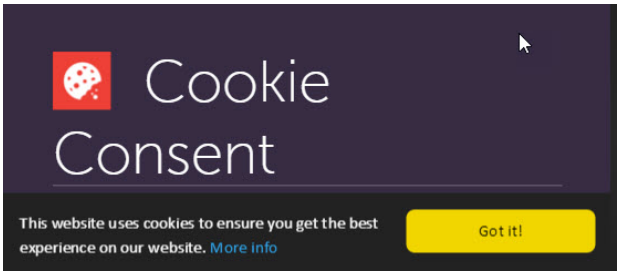


Figure 16: Cookie consent

In this example all choices are possible for the user, but by choosing 'More info' the user is redirected to a page with information about how cookies can be disabled, no information about specific cookies or functionality could be found. Clearly this is not according to several of the 5 fundamental principles presented earlier in this text. To be fully compliant with art. 7 in GDPR (Conditions for consents) the user should be offered a GUI with a specific No or Yes statement and the possibility to turn specific types of cookies on/off as seen in figure 19.

There is no specific requirements in GDPR 'regarding Cookies banners' but several interpretations and legal decisions like the Planet 49 case[47] and the ePrivacy directive[3] indicates that users need to be informed about both functionality and intensions of cookies before they are set.

A valid cookie consent banner must include the following features.

- All cookies must by default be put on hold until user consent is collected
- The information must be simple and accurate
- All cookies except necessary ones must by default be unchecked
- The web site must function properly even the user opt. cookies are turned of
- Consent from user must be collected and documented for further needs
- Consents must be updated regularly, i.e every 12 month

In the next step sites who offered a cookie policy and/or collected consents for the use of various kinds of cookies were inspected. This part of the study partly confirms the answers in the survey and initial findings, but we also see the presence of 3. part tracking tools. Figure 17 is a 'cookie insight report from Cookie Information Consent Management platform[64] as previously described in this chapter. In this example the specific lottery claims to have no 3. part cookies in the answer to the study, and had only a brief explanation related to customer tracking at their web pages. The name of the lottery has been removed.

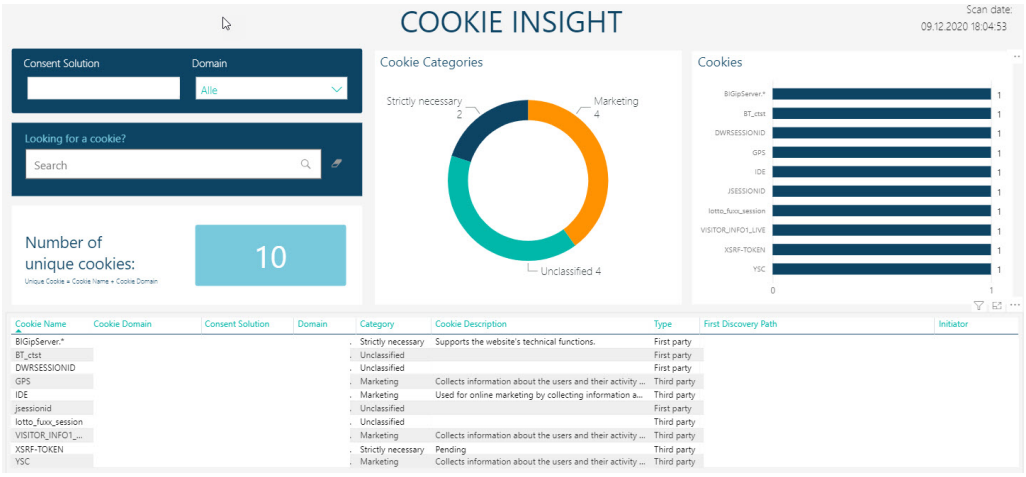


Figure 17: Cookie consent

The detailed scan result in figure 18 confirms the existence of 4 3. part cookies, and by inspecting the specific cookies used we typically find the GPS cookie used by YouTube to collect location data about the user

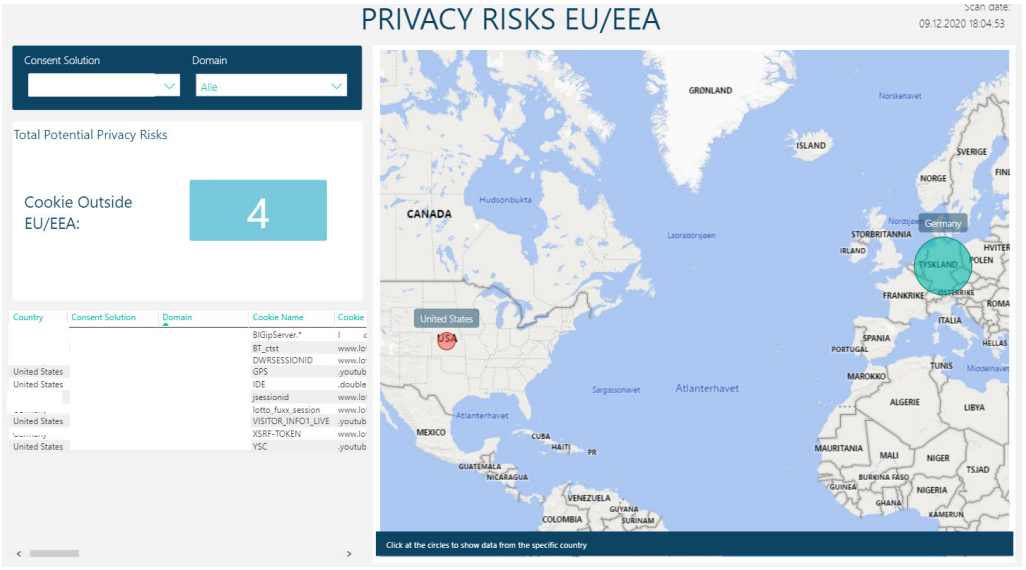


Figure 18: Data transfer

Geo data could be collected anonymously as single data sets and possibly not be considered as personal identifiable information(PII), but considering that the collection most likely will involve collection of related data such as device ID(IMEI number) making it possible to track specific devices, this is PII data. Considering that Geo data easily could be related to specific features such as home address or workplace etc., the amount of data collected also is important to be able to see patterns or and recurrences. If we consider this as PII data, a more interesting part of the report is that the collected data apparently seems to be transferred to USA. According to the Schrems II[8] conviction Privacy Shield[7] is no longer considered to

be a legal basis for transfer of PII data to the USA making a specific risk assessment necessary to evaluate if a sufficient legal basis and adequate security measures is in place(GDPR Chap. V). For this specific lottery no such information could be found. It has to be mentioned though that the web page was scanned several times and that the GPS cookie not was found in all of them. This explanation could be that YouTube is a typical free 3. part services typically used for presentation of videos for specific purposes and not as part of the ordinary web page functionality. Nevertheless, cookies were placed in browser without informed consent.

If we take a closer look at 3. part marketing cookies we find 41 different types, the most used ones are 'UID' from Adform and 'fr5' from Facebook. Adform is a global media advertising company, and according information published at their web site[65] the UID cookie is used to create a unique identifier. Several other cookies from Adform could also be identified, and according to 'Adform product and services privacy policy'[65] the legal basis for collection of PII data is either informed consent(obtained by customers) or legitimate interest(GDPR art. 6). By using Adform cookies the customer either needs to collect a specific consent or rely on a risk assessment etc. to document that the collection of PII data could be done with legitimate interest as legal basis.

Facebook needs no specific presentation, and according to independent cookie libraries like cookiedatabase.org[66], this specific cookie is used to enable ad delivery or re targeting as a part of the use of Facebook Pixel who integrates websites with Facebook functionality .
Facebook itself describes the use of cookies from a user perspective and has little or limited information about legal basis for the use of cookies[67]. Like Adform cookies this will then be user consent or legitimate interest

Using legitimate interest as legal basis could be challenging since the data processor would have to prove that the use of data actually is performed in a way that is expected by the user and has a minimal impact to the privacy of the individual objects. The Rigas case[68] documents that it's not enough to just decide that it is in your legitimate interest to collect and process PII, you also need to evaluate potential risks to individuals interests, rights and freedom according to GDPR recital 75[1]. Several independent public agencies like the British ICO(Independent Commissioner's Office)[6] refers to this process as a Legitimate Interest Assessment(LIA) involving three steps:

- **Purpose test** – is there a legitimate interest behind the processing?
- **Necessity test** – is the processing necessary for that purpose?
- **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?

In general, this process will help the data processor to both understand the processing of PII, document and avoid potential risks and finally demonstrate compliance with GDPR.

Several data protection policies examined in this study refers to legitimate interest as legal basis for cookies and tracking tools. An open question though is if the individual companies actually has performed a LIA and will be able to demonstrate compliance with GDPR requirements and the e-commerce directive[14] if requested by either customer or national data protection authorities.

By scanning web pages found 5 lotteries that used the 'UID and 'fr5' cookie were found. By inspecting them closer they all have some kind of information regarding the use of 3. part tracking cookies at their website, but again the quality of the information is questionable. A specific consent for the use of tracking/marketing tools could not be found

9 out of 22 companies in the survey offers functionality to disable or remove cookies from their browser. For the remaining this has to be done manually. This is no requirement or interpretation of the GDPR directive, but but if we consider the requirement related to consents this still could be argued. A consent should be possible to withdraw just as easy as it was given, and removal of cookies need to be included to make a withdrawal of a cookie consent effective and meaningful.

8.9.1 A cookie bias

A summary of all observations related to the use of cookies confirms a cookie bias. All 22 lotteries either participating int the survey or being a subject to closer scanning/examination fails to comply with the EU cookie directive[13] at some point. Only a few sites like fig.19, showing a screenshot from a company web site offers a almost perfect GUI for cookie consent management.

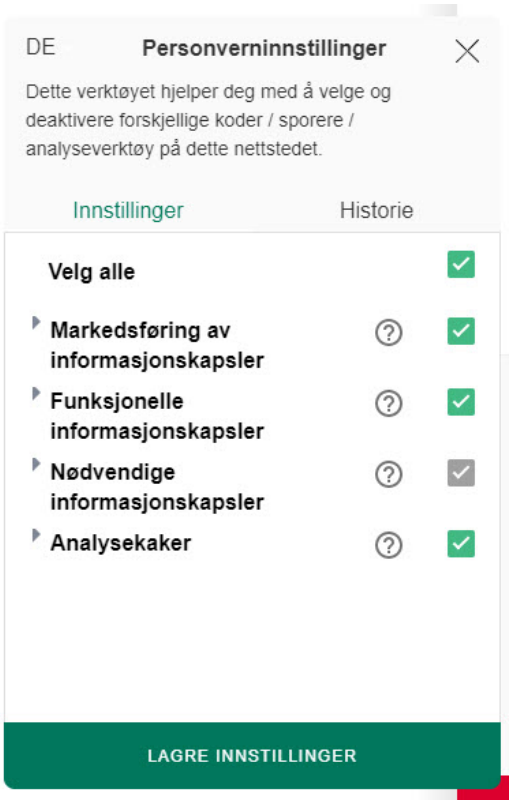


Figure 19: Cookie consent example

Unfortunately the choices have not been made opt-out as described in GDPR art.7 The provided information is written in a clear language offering the user to make a really informed

choice to accept or not.

The cookie bias as described in chap. 7.8 where we could see that customer were not informed about the use of cookies could be summarized as:

- **Not collecting a specific consent for 3 part tracking or marketing cookies** but still placing cookies in user/customer browser that collect personal data.(Placing cookies as an default operation without giving the user possibility to deny.)
- **Not providing specific/necessary and detailed information about the presence of tracking tools**/3. part cookies or other types of cookies before they actually are placed in browser
- **Not providing the necessary needs to make the customer able to remove his consent(if given)** . This makes it much harder to remove cookies than actually allowing them to be installed

All lotteries answering the survey is certified according to both ISO 27001[9] and the lottery specific WLA security standard[15]. For the remaining lotteries all are WLA SCS certified according to WLA web site who presents a comprehensive list of certified lotteries. According to the individual web sites a majority is ISO27001 certified and use the ISO 27001 logo/references on their web sites.

GDPR compliancy is mandatory for all data controllers handling PII data with only a few exceptions. According to ISO27001 control A 8.1 asset management and information classification is needed to provide both appropriate protection and maintenance. Further, information should be classified and procedures for handling should be implemented in accordance with information classification. This should involve both definition of ownership and rules for acceptable handling. This is similar to GDPR art. 30 who states that the data controller should keep record of all processing activities including 3 part/sub supplier handling and possible transfer of PII data. In case of transfer of data a sufficient level of protection needs to be demonstrated, this could typically be a data processing agreement(DPA) or other legally binding conventions.(GDPR Chap. 5) < It could be questioned whether data collected by cookies are PII or not, but as long as it involves collection of IP addresses and profiling it undoubtedly is to be considered as PII information under GDPR. This is also recognized by both national data protection authorities in Norway[5] and the UK[6] etc. who argues that a specific consent from the users is needed before cookies for marketing purposes is installed (ref. chap 6.8). Some data collectors strongly argues that pseudonymization of IP addresses where part of the address is replace by dummy data to create a non-traceable ID is to be considered as non PII. As long as the collector actually has hold of the IP address this hardly could be used as an argument since processing of PII according to GDPR both applies to collection, handling, and/or storage of personal data(GDPR art. 4 and recital 40).

According to EU(WP29 opinion 4/2007)[69], a natural person can be considered as “identified” when, within a group of persons, he or she is “distinguished” from all other members of the group. Device fingerprinting[63] could i.e. be used a a technique for user tracking/identification of online users based on their device characteristics and still be considered as PII under art. 4 in GDPR not involving use of IP address. Eckersley [70] found 99.1 percent correct identification of returning visitors to a web site by using browser characteris-

tics like system fonts, browser plugins etc. already in 2010. They even published a test side (https://coveryourtracks.eff.org/) to test individual browser protection from tracking and fingerprinting. Cao et al.[71] successfully identified 99.24 percent of users by utilizing OS and hardware features like graphic card, CPU and installed scripts in their study in 2017. In this study I found no documentation or information that could indicate the use or presence of browser fingerprinting tools.

The use of cookies for marketing involve both collection and transfer of PII data, and as we have seen several legislation's regulates the use of this kind of data. As a part of ongoing certification programs regularly audits and reviews is performed to assure that certified companies complies with the specific controls and security levels. It is though a controversy to see the lack of information related to the use of cookies and security requirements. We have seen that there seems to be a cookie bias for the companies in the study, but at the same time this is information that should be a part of asset/inventory lists and records of processing activities as described in chap. 8 of ISO 27001(A.8.1.3) and GDPR art. 30(Records of processing activities)

A discussion about why internal processes an audits fails to document this kind of handling of PII might be partially out of scope for this thesis, but from personal experience and exchange of experience with between lotteries in Europe a number of explanations could be given

- **Insufficient detail level** - Details about systems in use could exist, but insufficient or erroneous information could be collected to document what kind of data is collected and where data might be transferred
- **Inadequate knowledge about technical details** - Certain tools like Google Analytics etc. needs proper configuration to be compliant with GDPR, by default they might both collect and share PII. This is typically explained in Google privacy and security statements[72] as an option to mask IP addresses etc., but it needs to be requested and installed by the customer as a specific Java script. Other products like Hotjar and Clicky seems to provide the same options, but with a market share of 90 percent Google Analytics, it is by far the most used product in this category.
- **Internal differences** - Responsibility for both handling and documentation of tools for collection and use/handling of PII data might be split between several departments making it challenging to both ensure sufficient and effective distribution of information and/or data responsibility
- **Lack of knowledge to important laws and regulations** - Hardly an issues since booth GDPR and ISO 27001/27701 etc. both should be easy to access and understand and applies to all data handlers in Europe. Still, we see differences that might reflect cultural differences in Europe. We have seen traces of this difference in combination with the answer rate, but also the quality of data protection policies, consent management platforms seems to be better implemented in Northern Europe and/or in combination with the size of the lottery. This is qualitative interpretation of the study result that might be needing further investigation to either support or refute this hypothesis

8.10 Company certifications

As seen in chap. 7.10 and fig. 13 a majority of the lotteries are either certified according to the lottery specific WLA standard[44] or ISO 27001[9]. Both standards are comprehensive frameworks describing best practice with both lottery operations and information security in general. The WLA certification could involve both implementation of regular lottery controls and a more specific certification for responsible gaming.

Certifying to both standards involves both documentation of procedures, leadership involvement, risk assessment processes etc. and continual improvement with correct handling of both errors and deviations. A substantial amount of work is needed to get an ISMS(Information Security Management System) in place and kept up to date.

Is is paradox that so many choose to certify using both time and resources to prepare a certification process and at the same time shows little or missing transparency towards customers a.o. A few of the inspected presents the ISO logo, a larger number presents the WLA logo, but still far from all. ISO 27001 is by far the most known standard for information security, and a ISO 27001 certificate shows that the organization complies to with numerous regulatory and legal requirements that relate to the security of information and handling of PII. An interesting observation though is that VISA/Mastercard logo is used by a handful of lotteries to described offered payment solutions. These are well known brands with a high level of trust among users and could be referred to as payments standards.

Using the ISO and WLA logo actively would show a high level of integrity and show that the handling of information including PII is done according to best practice and regularly audited by an external auditor. This is supported by Metzger[25] who suggest that companies should examine how security should be communicated by using third party seals. Referring to standards in data protection polices etc. will not have the same effect since these documents tend to be both inaccessible and not easy to read as previously described in chap. 7.5 a.o. Displaying the ISO/WLA logo would be a more effective way to transfer this information than in writing.

8.11 Focus group interview

As presented the purpose of the focus group interview was to use the collected material from the interview to confirm the observations and analysis in the study or at least provide input to the study itself. In the previous chapter we learned that the members expressed concerns about the effectiveness and readability for data protection policies and cookie policies etc., they tend to be written more ore less to meet the needs for the data controller and not necessarily the customer or data object.

This pretty much confirms the observations in the study that shows great variation in information details, accessibility etc. for of the collected material. Important information like legal basis and collected personal data in general is either missing or explained in a misleading or difficult language.(ref. chap.6)

The use of cookies and tracking technology is by the members of the group explained as

not very accurate and possibly a risk since exposure of commercials and information about gambling could be both irrelevant and possibly be perceived as cynical by the customers. In the study we have presented a cookie bias where cookies are placed without customer consent and sufficient information(chap. 7.9.1.) The relation between the collected material from the focus group interview and the observations in the study seems to be related to knowledge and understanding, perhaps in relation with ethical considerations. The presented explanations for the 'Cookie bias' as presented in chap 8.9.1 is strongly related to the observations from the focus group interview and reveals a lack of skills and knowledge. Digital marketing tools like Google Analytics, Webtrends etc. is as already mentioned typical by default configured to collect a wide range of personal data and needs to be paramaterized to comply with collected consents and/or legal basis. This will require in depth knowledge about both installation and operation and perhaps not have sufficient focus when collection of customer data and customer behaviour data is the primary target.

As seen in chap 7.5 responsible gaming tools could be implemented as a different tools with variations in both language, timing and personalization. Studies like Blaszinsky et al.[37] and Auer and Griffits[50] show that they can both reach gamblers at different levels of risks and at the same time be effective. The result from this study reveals that several tools is in place as tools that give the customer access to data and loss/bet limits, exclusion from further gambling etc.(chap 7.4). Compared to AI and machine learning this could be considered as simple tools to implement, but still several members of the group consider them as highly effective. AI and machine learning has a potential to improve and complement responsible gaming tools, but as expressed by the group member this has concerns and risk related to ethical issues. We need to have a clear understanding of what we are trying to achieve and how. From my perspective I believe that this should be done by closely observe and analyse the effect from implemented tools and compare this with important business objectives and legal frameworks etc. For a monopolist and regulative perspective this would typically be to prevent or reduce different variations of gambling problems and even money laundry and illegal activities related to gambling.

9 Recommendations

In chap. 5 we defined the research question as

- What is the situation related to the use of TET and PET techniques in European lotteries,what kind of techniques are implemented and how.
- What are the differences between observations and expectations in laws, best practice/standards and ethics
- What will be the best recommendations to improve the current situation

The first two parts of the research question is answered in chap. 7.and 8, in this part we will suggest the following improvements and recommendations to provide answers to the last part of the research question:

9.0.1 An extensive data protection policy

Every data controller should present an updated and extensive data protection policy to document compliance with GDPR and basic data protection principles. The origin of the policy should be as described in GDPR chap. III with details about:

- **Legal basis** - Legal basis for data collecting with specific references to any presence of national laws or customer contracts.
- **Information about collected data** - Details about types of collected data, preferably described a table with both identification and origin of data
- **Contact details -** Contact details for data controller, data protection officer and national data protection authorities as a receiver of possible complaints.
- **User rights** - The right to rectification, deletion, limitations and protest to handling of PII and how the rights should be executed
- **Access to data** - Access to PII and data portability including a GUI for data export.
- **Profiling** - The presence of automated decision tools(Profiling) with specific references to RG tools. Technical information about how these tools are used with details about automated profiling and possible use of AI technology.
- **Protection of PII** - Protection of PII with references to technical and organisational measures including both retention rules and deletion of PII
- **Information about sub suppliers** - Information about sub suppliers and export of data to 3 parts and sub suppliers.

The data protection policy should be easy to identify and access on company web pages as a specific document named 'Data Protection Policy' or equal. It should not be a part of any other documentation of company preferences or activities. Optimal placement would i.e be at the bottom of the home company page. Related to gambling and the lottery industry a specific part of the policy should describe the use of Responsible Gaming tools(RG tools), this will be further explained in chap. 9.0.4

9.0.2 Access to customer data

Each data object should be given online access to own PII data with complete insight to origin of data and references to legal basis like customer contract, consent or national law. A copy of the correct version of customer contract should be available with any consents given. A platform for consent with easy access and equal possibility to give/withdraw consent should be present. Functionality for export of PII should be provided making it possible to export data to a readable format like Excel/CSV. PDF is by several data controllers used as export format, but considering the fundamental rights and understanding of GDPR art. 20 as data portability and data transfer this is not sufficient. PDF is basically impossible to convert or be read by other systems and will not meet the requirements of being structured, commonly used and machine-readable.

9.0.3 Cookies and customer tracking

In chap. 6 and 7 I presented indications of a 'cookie bias' clearly indicating a lack of information regarding the use of cookies and mechanisms for behavioural tracking. A recommendation would then be to implement controls and measures to avoid this bias. This should not only involve the use of cookies, but also handle all kinds of tracking tools.

Apple launched ITP(Intelligent Tracking Prevention) V2.3 in 2020 to restrict website owners and advertisers from cross-site tracking of their users. In practical therms, third part cookies are blocked an will typically be deleted in Safari. Google has stated that they will only sell targeted advertising based on first-party data i.e. data collected from consumer interactions with Google owned properties like YouTube, Google Search, Google News, Gmail etc... This will effectively prevent cross cite tracking as websites no longer can place cookies in Chrome for later re targeting or attribution etc. unless the user specifically have given a consent for this purpose.

New techniques like device fingerprinting and user consent to track users across web sites and devices could be introduced as an answer to ITP and similar techniques. These tools might be less known and less visible for the user calling for a higher level of details and information to the users.

As a result of this situation a specific cookie policy or a policy describing the presence of all kinds of tracking mechanisms should be presented at company web pages including:

- **The purpose** of user tracking
- **What kind** of data is collected
- **Legal basis** for data collection
- **A comprehensive and update list of cookies** as described in chapter 7.8 and/or other tracking mechanisms
- **How to avoid user tracking.** Web pages should be fully functional even though the user has not given his/hers consent to the use of tracking mechanisms

Regarding legal basis, using legitimate interest as basis could be challenging as discussed in chap. 8.9. If the data controller chooses to use this basis it should prepare and regularly update a risk assessment(LIA - Legitimate Interest Assessment) to demonstrate sufficient compliance level. It would not be required to present this assessment in a cookie policy etc. as

the information both could be classified and detailed. The organization should though be prepared to present this information to national data protection authorities and even by request from customers. A more recommendable way would to get legal basis for handling of PII would be to collect user consent, but as described in chap. 8.9 specific and detailed requirements regarding fundamental principles of collection and use of user consents must be followed.

Offering personalized information or personalized products to customer does not necessarily have to be e negative experience. Related to gambling and sport betting it is no secret that customers have favourite teams and favourite sports events. Offering a personalized user experience could be a positive and desirable product, but it has to be offered in a clear language with a level of details making it possible for the customer to understand the benefits and consequences of a consent.

Several suppliers like Cookie Information[64] and Onetrust[73] offers software tools that can be integrated with web pages and offer technical capability to inform visitors about the types of data they collect and ask for their consent for specific data-processing purposes. This could be beneficial for companies that would like to outsource this activity to a professional partner instead of using internal resources to develop and maintain their own consent management solution. The negative consequences would be loss of control and possibly inability to make rapid corrections and specific company adaptions. A question would also be whether the specific software supplier complies with important data protection features like secure transfer and storage of data etc. This would still be the responsibility of the data controller and needs to be addressed through a risk assessment and possible use of a data processing agreement.

Other interest group like The Interactive Advertising Bureau (IAB)[22] is preparing a framework that will help the digital advertising industry interpret and comply with EU data protection requirements. By using this framework, a centralized consent management platform will be accessible for multiple sites allowing the consent to be used across both sites and devices. This could also be an alternative for user profiling and commercial marketing.

From the focus group interview we learned that concerns related to ethical issues and customer tracking is an issue, and my recommendation is that this should be addressed as a risk together with other risks. A typical risk in this context would be possible loss of reputation, but lawfulness should also be considered. A typical risk reducing measure could be as discussed in the focusgroup interview to avoid using these kind of tools since the risk of being perceived as both cynical and irresponsible i highly likely.

9.0.4 Use of RG tools

If we take a closer look at the presentation of feedback from Playscan in figure 14 and 15 in chapter 8.5, an answer to negative feedback(and those that tries to explain the result of the test as well) would be to offer even more information and transparency. This should be reflected both in personal messages and more general information like Data Protection Policy and Customer Contract etc. Timing is also important, and since important sports event seems to trigger more complaints/feedback perhaps intensified information campaigns in these pe-

riods would be appropriate.

After inspecting several data protection polices and/or customer contracts it is also a recommendation that information related to the use of RG tools should be presented as separate information and not as a part of a more general information about collection of personal data etc. This will emphasize the meaning and importance of RG tools and be an answer to the lack of understanding and qualitative/personalized feedback... A qualitative approach is important since players tend to be both offended and showing lack of understanding when RG tests/tools are made mandatory as seen in chapter 8.5[60]. This study clearly show the need to both show transparency regarding why these tools are used and what the intentions are. This needs to be presented with a clear and neutral language. An observation from interviews with high stake players in this study clearly indicated that 'classification' or a 'judgemental' approach not created positive attitude among the interview objects. If the given information in the interview was neutral and explaining, the participants replied that they 'thought it was OK'

The use of RG tools is strongly connected to expectations and regulations from public authorities. This would typically be a specific legal basis for handling of PII and mandatory time and loss limits all stated in a customer contract. Legal basis for personalizing and customer tracking, newsletters etc. on the other hand is based(or at least should be based) on customer consent calling for additional information about the freedom to choose, the possibility to withdraw consent etc. This need to be clearly reflected in both customer contract and data protection policy etc. It should be clearly stated that certain/specific RG tools are either mandatory or voluntarily clearly separated from information about personalization and user tracking for commercial purposes.

Several of the studies presented in this text presents a user paradox where initial use of a self diagnosis tool will be followed by non repeating use. At the same time the same studies identifies these kind of tools as a effective method to provide insight to personal behaviour and give advise based on personal patterns[37]. A way to bridge this paradox would be to improve the methods of feedback, including both frequency and method[61] Forstrom et al.[74] presents Playscan status as a total risk level for individual customers calculated on basis of night owling, chasing losses and total spending etc. The individual customer will the be categorized as typical green/red/yellow category with individual RG tools like personalized feedback for each group. This is s static computation of an overall risk level at specific time, but it misses some important parameters like time, a genuine on to one relationship with the customer and real individual feedback for single/specific users. The calculation model would also have to be re-calibrated or re-designed regularly to reflect changes in games, stake etc.

To improve the identification of patterns and behavioral related to problem gambling and gambling addiction I believe that artificial intelligence and machine learning could be introduced to identify multiple patterns for user tracking and user feedback. Instead of having three possible models for customer classification, we could have multiple models each with individual feedback and types of personal messages.

A pretty common understanding of AI technology is the ability to process large amounts

of data and recognize specific patterns and objects. As presented by IBM[75] AI technology is based on neural networks with the following levels:

- **An input level** where data enters the network - In this model this would be gambling transactions with loss and wins, transactions etc.
- **At least one hidden level** where machine learning algorithms process the inputs and apply weights, biases, and thresholds to the inputs - At this level the model should compute individual feedback/recipient groups based on gaming rules and loss/bet limits etc.
- **An output layer** where various conclusions—in which the network has various degrees of confidence—emerge - The final result should be a model where feedback to individual customers are presented on a individual level.

Fig. 20 show the relationship between Artificial Intelligence, Machine Learning and Deep Learning The model suggested in this study would be a problem solving mechanisms cate-

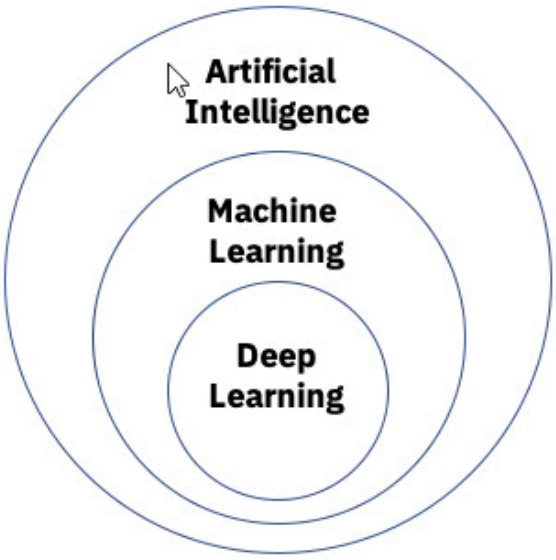


Figure 20: Artificial Intelligence model

gorising customers/players with basis in purchases/transactions and static parameters like bet/loss limits etc. This would be basically be a traditional AI model that could trigger specific feedback to specific groups based on historic values and interpretations of bet/loss values, spent time on gambling, channel etc. as suggested by Auer/Griffits[50]. The feedback messages would be based on human interactions and parameter setting. A far more advanced version of the AI model would involve Machine Learning algorithms where a program code is given the possibility to learn from itself and perform specific tasks with increasingly accuracy and detail level. This model would still involve some kind of human interaction/input, but would be a predictive model with the possibility to predict possible future gambling problems. Increased loss or playing duration etc. would then be indicators of a possibly rising gaming problem, not just an indication of limitations related to bet/loss limits etc. Feedback messages would be fully or even completely automatized providing a wide range of individual analysis and individual message structure/language. A typical parameter for classification/analysis

could be future sports events as described in chap 7.5 that could trigger feedback related to possible future overspending and gambling problems

A model based on Deep learning where even more self learning/training and a total absence of human interaction is introduced would be out of scope related to the use of RG tools. Interaction with customers and identification of possible gaming problems/addiction would always need to involve some kind of human interaction and analysis at different stages. Typically individual players will have a need to be offered professional help or even individual stake/bet limits or possible exclusion from gambling for a period of time.

Introducing AI technology would rise both juridical and ethical issues that needs to be addressed. These techniques are far more advanced than traditional RG tools, but at the same time Data Protection Policy and Customer Contract etc. needs to show the same high level of transparency related to collection of data, tracking of customer behaviour etc. as with ordinary RG tools. There could also be issues related to technical risks like data sharing/transfer and access to data if we use 3. part suppliers/tools etc. Detailed customer tracking and collection of PII data could also rise specific ethical questions like the level of influence/impact to human freedom/human rights and the need to regulate and control gambling.
GDPR art. 22 specifically prohibits the use of automated profiling and calls for a specific legal basis for this type of decision making. This clearly indicates that any information given about these kind of tools/processing needs to be stated in a clear and easy understandable language with references to legal basis.

9.0.5 Updated asset list and records of processing activities

In chap. 8.9.1 we discussed the connection between asset management as described in ISO 27001 and record of processing activities as stated and required in GDPR. A recommendation would be not just to comply with GDPR regarding process activities, but also combine this with asset management. Asset management as described in ISO 27001 A 8.1.1 not only involves software/hardware, but also infrastructure and services that could involve processing of PII. It would be a natural approach to categorize information in information classes like customer data, employee data etc. and map these to specific assets. Processing of PII could also very well be related to physical handling of documents and not just digital information handling.

Datatilsynet[5] has suggested a template to keep record of processing of PII, but this template tend to be to simple to involve asset management and needs to be improved to serve this purpose. It could be possible to use a specific software like 'ISMS Secure' or 'ISMS online', but again, the challenges still would be related to the quality of the data and not the specific system in use. Creating a inventory/asset list and record of processing activities would be a limited task, keeping it updated and living would is far more challenging. Routines and guidelines needs to be in place with dedicated ownership to processes and activities. This should involve definition of relations to important information owners/sources like CMDB(Configuration Management Database) and license management tools. These are the places where we will find records of software in use/expired software and a updated picture of running services and processes. A CMDB could be a way to document processing of PII, but the purpose and nature of these tools are not necessarily compatible with the flex-

ibility and scalability needed to both establish and maintain an updated asset list and record of processing of PII as described in GDPR. Details about hardware components would not fit into a list of processing activities, and licenses for software might be necessary to generalize into specific groups like data storage or data transfer.

An update asset/processing list not only will be helpful to comply with regulations and laws, but would also be a natural origin for internal/external audits as described in ISO 27001 9.2. If we involve asset classification as described in A 8.2.1 it would be easy to classify assets and create audit plans with a risk based approach, typically audits to reveal non conformity's in important software tools or business services related to information security

9.0.6 Anonymous disclosure of data

In chapter 7.7 we discussed several national and EU legislation's like protecting of both whistle blowers and anti money laundry. A final conclusion from this chapter is that legal requirements calls for the use of a specific channel for anonymously disclosure of data
Using a 3.part as described in chap. 3.7 would be a way to increase trustworthiness through protection of personal data. To be truly effective anonymous disclosure of data should involve a 3. part to make sure that any person who reports breaches and non-compliancy would be fully protected and not a victim to retaliatory measures. This should not only involve the reporter himself, but also facilitators, colleagues or relatives of the reporting person who are also in a work related connection with the reporting person's employer or customer or recipient of services as described in chap. 41 of the directive[51]. The 3. part should be able to offer:

- **Confidentially** - Meaning that correct depersonalized/anonymized information should be handed over to to the client or legal authorities if required. Only the 3. part should know the identity/origin of the data. The reporter should be offered complete anonymity and protection against any means or efforts done to reveal his/hers identity
- **Integrity** - Meaning that the data should both be collected and stored in a way that will provide protection from manipulation, deletion etc.
- **Accessibility/Availability** - Meaning that only those who are entitled or trusted should have access to collected data.

The company could off course offer this service as a part of their ordinary operations, but it would easily be questioned how strict demands for information security(Confidentiality, Integrity and Accessibility) could be met and documented. A finale recommendation would be that this needs to be done by a 3. part to ensure both transparency and trustworthiness.

9.0.7 Use of additional PET/TET techniques

In chapter 3 we discussed the use of PET(Privacy Enhancement Tools) and TET(Transparency Enhancement Tools) and presented a list of PET/TET techniques implemented in lotteries. Article 32 in GDPR states that both processor and controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. To accommodate this GDPR requirement, specific technical features related to data protection needs to be evaluated at regular basis. Encryption of data in transit or at rest is mandatory requirements, but for further improvement such evaluations also should consider encryption

of data in use. Art. 25 in GDPR states that data protection and privacy should be implemented by default(Privacy by design). A recommendation could be that this is done one in two ways.

Internal privacy enhancement

Data at rest in databases like datawarehouse etc. are traditionally secured by access controls and encryption. Having access to one specific record could the grant users access to complete data sets. Encryption techniques could be introduced to ensure that a minimum of data is revealed to external users. This will involve PET techniques like

- **Homomorphic encryption** - This allows data to be processed while still encrypted. Customer data could then be processed by software/users without showing the data in real time/unencrypted
- **Differential privacy** - This will ensure that no no individual in the data set can be re-identified. This can typically be implemented in large data sets like analysis on data in Datawarehouse(DWH) where only a subset or extract of collected data material is needed.

External privacy enhancement

In chapter 8.0.3 different techniques was presented for consent management, typical by a trusted third part. This could be further developed and include transfer of data to specific third parts, time of deletion(return of data) and mechanisms for enforcement etc. For the gambling industry this could involve transfer of data to specific sub suppliers or even use of personal data for research(Transfer of personal data to research institutions). The individual customer could be given the possibility to negotiate therms and enforcement of data handling conditions. I practical terms you could be given the possibility to decide(and be informed) about participation in research projects, decide not to disclose specific personal data or even decline transfer to specific sub suppliers. Some practical problems needs to be solved since a minimum of personal data is needed to participate in lotteries and the fact that denial of data transfer to sub suppliers might mean that specific products would inaccessible.

As a data controller specific measures could be implemented to ensure that enforcement of implemented techniques for data protection is documented for the customer/data object. At least to some extent it should be possible to increase the possibility to remotely audit implemented features by giving access to or reveal information about:

- **Audit logs and reports** documenting when and where data is transferred, deleted etc. Documentation of deleted PII after termination of a customer relationship would be of specific interest.
- **Logs from internal systems/processes** showing steps like winner selection, prize pay-out etc.
- **Technical details** like presented tools for internal privacy enhancement.
- **Consent managementt** as all ready presented

It has to be emphasised that information both should be given in a clear and understandable language and at the same time not reveal business critical information.

At the same time it could be argued that some PET tools are considered to be to complex by average users and as a result of this not will be trusted or give the protection they claim to

do. The privacy officer of Canada[76] i.e typical states that there is some basis for this skepticism, but at the same time the potential in these tools to provide controls and protection of personal data is highlighted as important.

I finale recommendation would be that a continuous evaluation of PET/TET techniques is needed to evaluate both effectiveness and suitability.

9.0.8 Data handler qualification and skills

In chap. 8.9.1 I presented inadequate knowledge about technical details as a possible cause to the cookie bias presented in this chapter. A high level of knowledge is a key factor to success calling for allocation of both focus and resources. As described in ISO 27001 chap. 5, leadership involvement is crucial and needs to be demonstrated

A recommendation is that this should be done as a cross section/company activity in a planned manner involving not only training and upgrading of skills but also:

- GAP analysis to reveal discrepancies between GDPR articles and company processes/procedures
- Proper training of staff at all levels
- Establishment and maintenance of necessary documentation
- Audits to evaluate the effectiveness of implemented procedures etc.
- Continual service activities to ensure adaption of processes and documentation to changing needs and demands.

The extent of a plan must be adapted to the individual organizations needs and guidelines. At the present time ISO 27701[12] might be the the most relevant framework to use.

Art. 42 i GDPR calls for establishment of data protection certification mechanisms. My personal believe is that a ISO 27701 certification could be a way to document a high level of skills related top handling of PII and would be a effective way to transfer this information to customer a.o.(ref. chap 8.10)

Specific interest should be paid to the use of a systematic risk based approach to handling of PII since GDPR clearly stats that a DPIA(Data Protection Impact Analysis) is needed for processing of specific types of personal data.(GDPR art. 35) The organization needs to develop procedures and knowledge describing how and when this should be done.

ISO 27005 typically will be an framework for risk identification and risk handling, but the data handler should establish their own threat register related to data protection to streamline this process. ISO 27005 only briefly suggest examples of threats, non of them related to data protection. From the presented topics in this text we have seen that relevant risks related to data protection will be:

- Risk of insufficient knowledge to software and methods for data collection
- Risk of not having legal basis for collecting and handling of PII
- Risk of not having updated records of processing activities and assets
- Risk of not presenting correct information in data protection policies, cookie policies etc.

- Risk of not offering customer/data objects access to own PII
- Risk of not having sufficient security for PII(Confidentiality - Integrity - Accessibility) including data transfer to third part suppliers.
- Risk of not keeping an updated risk register/picture related to the handling of PII.
- Risk of not having retention rules in place and not delete outdated/obsolete data

Methods for risk treatment and risk acceptance criteria also needs to be addressed and coordinated with company risk handling guidelines and procedures.

Blockchain and transparency

It could be tempting to recommend the use of block chain technology to store both transactions with price payouts and contract details for customers in av distributed ledger or block chain. Any user or node in the chain would then be able to see all transactions providing ultimate transparency related to prize calculation and prize payout. Distribution of updated customer contract would both be efficient and fast since we could relate this to smart contracts for each purchase or bet, and bet payments will be automatized.

There are though some major concerns that makes it unlikely that this kind of technology should or could be used, at least in short term. A fundamental right described in GDPR is the right to be forgotten as described in art 16 and 17. Since no part of a block chain actually can be deleted it will be impossible to be GDPR compliant, at least until a sufficient technical solution is in place. There will also be issues related to identification of data controller and data object if we do not know the identity of the parts in the block chain.

The fact that block chain/crypto currencies like Etherium and Bitcoin basically is anonymous or offer pseudo anonymous payment channels makes it impossible to control the identity of the player or the actual origin of the payment. Once a dirty cryptocurrency is in play, criminals can use an anonymization services like Tor etc. to hide the fund's source, breaking the links between bitcoin transactions. This will be challenging related to both anti money laundry controls and even responsible gaming tools.

Block chain technology is a relative new technology, and it could be that we will see technical solutions or clarifications that will solve these challenges in the future.

According to numbers from Norsk Tipping about 20 percent of weekly customers still makes their bets through av physical retailer. Even though this number is dropping over time a substantial amount of the customers almost never interact via digital channels. It is highly unlikely that customer contract and contractual provisions could be communicated fully digital for these customers, at least in short terms.

10 Validity and Reliability of the Study

In chapter 5 we presented the research question as a mapping of PET(Privacy Enhancement Techniques) and TET(Transparency Enhancement Techniques) techniques to enhance trust and willingness to share personal data both from a general perspective and a lottery/gambling perspective. Further we presented an assumption that some techniques might be more effective than others and what will be the most effective way to create transparency related to collection of personal data.

The result has showed us that there seems to be a lack of quality in the different implemented techniques and how they are presented to the users. The validity of the findings I believe allows us to make reasonable conclusions about both transparency techniques in general and techniques that are unique for the lottery business.

In chapter 5(Methodology) the internal and external validity was discussed, and it was argued that this would be high for both. Now that the final result of the study is ready it has to be discussed if this is correct or not, what is the real validity of the study?

10.1 Internal validity

Internal validity is only valid to the extent of investigation of a cause and effect relationship between treatment and outcome, and a study will have a high internal validity if the discussed relationship cannot be explained by factors outside the study. This study more ore less based on observations from other studies with a qualitative approach to implantation of described privacy enhancement techniques. The result from these studies are well documented with a high level of internal validity that strongly supports the observations and discussions presented in this thesis. The collected material in the study itself does not reveal a cause and effect relationship, and even though the validity of the data is relevant, the internal validity is limited since no cause and effect relation is investigated in practical terms.

There are other effects and facts that could question the overall validity as well. Since the introduction of GDPR in 2018, compliance with this legislation have been widely discussed in media with reference to heavy fines and loss of company reputation. In chap. 8.9 we saw a bias between observations and reported use of cookies. This effect could be explained as the 'Hawthoren effect'[77] where people tend to change their behaviour when they know that they are observed. Giving a slightly positive answer to the questions in the survey would be tempting since this would give a better impression of the company or even reflect what the respondent really wants the answer to be. By using at specific tool or doing a manual inspection of the individual web pages this effect partially has been minimized, at least for some parts of the study like data protection policy and the presence of tracking tools like 'cookies'. For these observations we have not just relied on reported material from the participants in the study, but also verified whether they are plausible or not. This has documented

a cookie bias(chap. 8.9.1) and revealed what might be the the most likely explanation to the observation. As a result the internal validity will be increased.

On the other hand we have seen the presence of other dependent variables that would influence independent variables like presented TET/PET technology. A typical example would be culture as presented in chapter 8 where we discussed the differences in answer rate. Another example could be general maturity related to data protection since specific parts of northern Europe have a longer history of data protection laws than countries in the southern parts. In chapter three we presented data protection legalisation's in Europe in a historical perspective with references to national laws back to 1970 for the Nordic countries. At the same time OECD(Organisation for Economic Co-operation and Development) presented a set of international data privacy and protection guidelines in 1980, but only as a voluntarily non-binding framework. The problems with differences between different data protection laws in Europe was not solved before 1995 with the EU's 1995 Data Protection Directive 95/46/EC[78]. Before this data protection in Europe was a patch work of regional data protection requirements, and could at least partially also explain differences in the observations and collected data. Both culture and maturity level could be considered as confounding variables that will be difficult to both control and evaluate the impact to the validity of the study.

Dependent variables like already mentioned TET/PET technology are better controlled and documented in the study, and we even supported the findings with additional observations from a focus group interview. This will have a significant impact to quality in the collected material and the overall validity.

As a result it could be argued that companies and countries with a long term relationship to data protection and legal requirements have a better understanding of possible benefits while others again might see this a non productive and needless governmental involvement. The result could be differences in both answer rate and the quality of the answers. To increase the internal validity and increase the probability that the presented observations and recommendations actually presents the most likely explanations I believe that the following changes could be done to the study

- **Replace the questionnaires with interviews** - Instead of using a non personal questionnaire, personal interviews with the recipients could have been prepared. This would ensure that the questions where correctly understood and open up for follow up questions in case answers where incomplete or lacking important information. A personal one to one relationship would also be beneficial for the answer rate. A possible negative consequence of conducting personal interviews could be that one person might not be able to answer all questions in the survey. By using PDF questionnaires multiple persons could answer and possibly use longer time to collect the necessary information
- **Collect data from multiple sources** - By increasing the amount of collected data material I believe that the overall quality of the study would have been improved and given a higher confidence level to the collected observations. The overall answer rate presented in chap. 7 is low, and an increased level on collected data is needed to increase the internal validity. A possible measure could i.e be to perform focusgroup interviews with customer to collect user stories etc.

10.2 External validity

External validity refers to the extent to which the results in a study is valid for situations beyond the study itself. Like other businesses the lottery business has its own internal regulations and frameworks, but as we have presented in this study it also relates to common legislation's like GDPR and ISO 27001 etc. Even though the answer rate tends to be low as discussed in chap 7., the external validity still could be considered as relevant. Observations are collected from real life settings, and there is no reason to doubt that lotteries relates to data protection and privacy in the same way as other industries. We have seen possible cultural differences, but still the use of PII data would be relevant in another context.

As already mentioned the focus group interview resulted in collection of additional data that we used to improve the validity and quality of the study

The low answer rate could though question the quality in the research since this could mean that we are missing sufficient data material to support or disprove the findings. To increase the external validity the same actions as presented for internal validity would be recommended to increase the amount of representative samples.

10.3 Reliability

Both validity and reliability reflects the degree of errors and failures in observations. GDPR states quite detailed how collection and use of PII is supposed to be done to be compliant and lawfully. This makes it possible to collect unambiguously observations of specific features like legal basis for collection of PII, collected data export of data etc. Other issues like the content of Data Protein Policies involves a bit more qualitative involvement for the observer, meaning that there could be issues related to consistency for some groups of observations. GDPR clearly states the needed specific information types that the data object is supposed to receive, but still there could be different understandings from one person to another on how this should be presented and and what it should look like. This is supported by the observations in the study that shows variations and differences for typically features like Data Protection Policies and the use of consent for cookies.

Since the introduction of GDPR in 2018 a great number of clarifications and guidelines related to understanding and use of this framework has been presented. This has clarified the needed efforts to be compliant and made it easier to reveal non-compliancy. For some issues like use of cookies and tracking tools it still seems to exist different interpretations and understandings even though correct use is presented by both National and EU data protection authorities like Datatilsynet[5] and the EU cookie directive[13]. The explanation could be unwillingness to change established procedures, but heavy fines and possible loss of reputation would be intensities to speed up this process and reduce this effect. Another typical example would be ISO27701[12] that provides guidance on how to comply with GDPR as an extension of a established ISMS(Information Security Management System). ISO 27701 maps the different GDPR articles to specific ISO27001 controls, but partially misses practical approach to implementation with examples and guidelines as ISO27002[79]. For organizations not using ISO 27001 or having a ISMS in place the suitability will be limited. A suggestion for further work would be to investigate this matter and suggest practical guidelines and implementation of

controls to be compliant with GDPR. This could involve at ISO 27701 certification without having an ISMS in place or even having a limited ISMS/ISO 27001 implementation i place as an origin for a ISO 27701 certification.

A summary of issues related to reliability would be that this could be considered as overall good:

- Collected data could be considered as reasonable accurate. We even introduced methods to reveal biases and contradictions in the collected material(Automated tool for cookie verification, manual inspection of data protection policies etc.)
- We have collected a significant and representative amount of data.
- Data are collected from different reliable sources like questionnaires, automated tools, manual inspections and focus group interview

Both validity and reliability in collected material could also be questioned in relation with the use of 'cookie information privacy management platform' as described in chapter 8. To increase both validity and reliability additional and similar tools could be used together with a more extensive use over time. This would give a more supplementary data material for analysis and deeper conclusions. Still I believe that the collected material will be sufficient to make the conclusions and support the hypothesis presented in this study

As a result of both high level of validity and reliability the number of errors in the collected material will be limited and offer a qualitative sufficient level to make conclusions and answer the research question as presented in chap. 5. I also believe that the collected material and following conclusions will be transferable to other business operations and data controllers since they all relate to the same privacy framework(GDPR) and need to offer equal solutions as data controllers to be compliant. Questions though could be related to the amount of collected material and answer rate. This is a major concern in the study with impact to both validity and reliability.

11 Conclusion

The collected material and laws and frameworks presented in this study is a comprehensive presentation of data protection and transparency in European lotteries. We have seen that a number of privacy concepts and theoretical models could be used to explain customer behaviour and how trustworthiness could be increased by utilizing these techniques. If we neglect them, the effect could potentially be devastating to a company reputation.

To answer the first part of the research question we have analysed the collected data and discussed what impact a low answer rate could have to the final result of the study. To compensate for this effect we have introduced measures like manual inspection of company web sites, automated analyses and focus group interview to create a sufficient database for analysis and recommendations.

Finally we identified a number of risks related to data protection and introduced specific recommendation to improve the current situation and address the last part of the research question

The finale conclusions from the study could be summarized as:

- **Identification of important differences related to interpretations of data protection laws(GDPR)**
    - Even though GDPR is a quite complementary presentation of rights and responsibilities related to data protection the observations show great variations related to fundamental data protection principles. Required information seems to be missing in Data Protection Policies etc., and important functionality is not available for the customers. Some observations might indicate cultural differences while others could be be explained as differences between a monopolist or having several competitive lotteries in the same market
- **Documentation of a cookie bias**
    - The most difficult and perhaps most controversial part seems to be customer tracking and the use of third part tools to collect customer behavioural data. Even though GDPR clearly states that legal basis is needed before any collecting of personal data related to profiling is initiated, the observations in the study show us that this might not necessarily be correct. The study has revealed a cookie bias where cookies are either placed without customer consent or required information is not given in a clear and understandable language. All participating lotteries in the study is certified according to ISO 27001, still they seem to fail to include these activities in their asset and inventory lists and records of processing activities.
- **Transparency is an important responsible gaming tools**.

- Personalization, timing and use of traditional TET/PET tools can be utilized as effective RG tools. As set of recommendation is presented to show how transparency and trustworthiness can be achieved by using PET and TET techniques. Simple PET/TET techniques like access to personal data might have a good effect, but more advances methods like Artificial Intelligence(AI) and machine learning could be used to improve these methods even further.

- **Identification of risks and recommendations**
  - A number of risks related to handling of PII is identified together with recommendations for improvement. Presented risks could be used as an origin for a company specific risk register related to handling of PII. The recommended improvements could be used to reduce both impact and likelihood related to identified risks

11.1 Further studies

The study partially has revealed a lack of standards and frameworks related to collection and handling of PII. This could explain some of the observed differences, and both meaning and understanding of important parts of GDPR and related legislation's still needs to be improved

This could be improved by i.e. further development of the IS27701 standard to meet the expectations of certification mechanisms for handling of PII as presented in GDPR art. 42. It should i.e. be possible to certify to the ISO 27701 standard without having a complete ISMS in place. Further studies could involve how this could be done for even smaller organisations and still maintain a high level on information security

Further studies could also involve development of best practice standards and guidelines for implementation like ISO 27002 and even different data protection certification mechanisms like the ISO 27701 standard.

Specific attention should be given to the development of new and improved methods for responsible gaming. Modern tools like AI and machine learning could show great effectiveness, but at the same time challenge understanding of laws and frameworks. Both investigation of new technology and how they can meet company and governmental requirements and expectations is needed.

A risk based approach is needed to handle PII effectively. Future studies could also involve how lotteries(and other industries in general) could develop a risk frameworks and utilize a predefined framework for risk assessments related to data protection.

12 Appendix

12.1 Questionnaire

My name is Bjørn Inge Sletta, and I'm writing to you as a part of a master thesis at NTNU(The Norwegian University of Science and Technology in Norway). Some of you might recognize me as a security advisor working for Norsk Tipping in Norway and also a member of the operational risk and assurance working group in EL(European Lotteries)

The reason why I'm writing to you is that beside my work at Norsk Tipping I'm also a last year student at NTNU finishing a master study in information security. As a part of this study I'm writing a master thesis about data protection and data transparency.

Your contact details has been collected from open sources like wep pages and/or participation lists from seminars etc.

I will would be very grateful if you could use a couple of minutes to answer an survey related to processing of personal data in European lotteries.

The idea of the study is to show the relation between increased customer trust and level of data transparency. This will be done by investigate the current situation regarding privacy and transparency enhancement and suggest effective ways to increase customer trust by increasing customer control with personal data.

The relevancy of the study is strongly dependent on the amount of collected material, making it crucial for me to have as many respondents as possible. The questionnaire is in the form of a PDF document making it possible to collect answers from several sources/recipients over a period of time in the same company.

The data will be handled anonymously with no reference to company or personal details besides company characteristics as shown in the survey. The collection of data is also approved by the NSD(Norwegian centre for research data) and data collected in the survey will be deleted or anonymized after the study has ended.

If you have question's, please do not hesitate to contact me on:

E-mail: bjorn-inge.sletta@norsk-tipping.no
Mob: 0047 95 98 14 26

Thank you so much for your contribution

Bjørn Inge Sletta

DATA PROTECTION SURVEY

The participation in the study is voluntarily. By participating you accept the terms as described in the survey. You may withdraw your consent at any time by contacting Bjørn Inge Sletta as responsible for the study, collected data will then be deleted

Please return the completed document to bjorn-inge.sletta@norsk-tipping.no

GENERAL INFORMATION

Company name

Company nationality

Number of individual customers

Number of employees

Company wep site

LEGAL BASIS FOR HANDLING OF PERSONAL DATA

What is the legal basis for the collection of personal data from customers in your company?

- ◯ Customer contract
- ◯ Customer consent
- ◯ National law
- ◯ Other, please elaborate

Is the customer contract or equal information about terms for data disclosure available at company home page??

- ◯ Yes
- ◯ No
- ◯ Only at innitial registration

What kind of customer data is collected

- ☐ Name
- ☐ Address
- ☐ Phone
- ☐ Email
- ☐ Bank account number
- ☐ Social security number
- ☐ Other, please elaborate

Additional consents collected?

- ☐ SMS communication
- ☐ Email communication
- ☐ Personalization
- ☐ Other, please ealborate

ACCESS TO CUSTOMER DATA

Does the company offer online access to personal data collected from the customer?

◯ Yes ◯ No

In case yes, what kind of data is available?

☐ Personal data related to the customer(name etc.)
☐ Ticket information(transaction data etc.)
☐ Prize and winner information related to the specific ticket/customer
☐ Money transactions
☐ Other, please elaborate

Is the cutsomer offerred the possibility to correct errors in personal data online?

◯ Yes ◯ No

Is the cutsomer offerred the possibility to cancel purchased tickets online?

◯ Yes ◯ No

DATA PROTECTION POLICY

Does the company offer a dedicated data protection policy at company home pages

◯ Yes ◯ No

In case yes, what kind of information is given in the data protection policy?

- ☐ Identification of data processor
- ☐ Contact detalis for data protection officer
- ☐ Purpose for the collection and processing of personal data
- ☐ The right to access personal data
- ☐ Deletion or anonymization of data(retention rules)
- ☐ Right to data portabillity
- ☐ Right to lodge a complaint to national data protection authorities
- ☐ The use of sub suppliers/recipients of personal data
- ☐ Name of sub suppliers
- ☐ The existence of atomated decission making - profiling
- ☐ Other, please elaborate

DATA PROTECTION OFFICER

Has the company appointed a dedicated data protection officer?

◯ Yes ◯ No

ANONYMOUS DISCLOSURE OF INFORMATION

Does the company offer a the possibility for anonymous disclosure of information related to i.e. warnings about money laundry or other possible illegal activities related to their operations?

◯ Yes ◯ No

INFORMATION ABOUT DATABREACHES OR UNINTENDED DISCLOSURE OF PERONAL DATA

In case of a data breaches or unintended disclosure of personal data, who will be informed?

☐ National data protection authorities(If required)
☐ Customers involved
☐ General information to customers on company home pages
☐ Other, please elaborate

HANDLING OF SUB CONTRACTORS

Does the company have a specific policy or guidelines regarding sub suppliers, data processing and the use of data processing agreements?

◯ Yes ◯ No

Does the company have a company specific data processing agreement used for data transfer to sub suppliers

◯ Yes ◯ No

USE OF COOKIES

Is a specific policy or declaration for the use of cookies available at company home pages?

◯ Yes ◯ No

Will a cookie consent message be displayde to visitors at company home pages?

◯ Yes ◯ No

What kind of cookies is used?

☐ Necessary cookies - For website functionality
☐ Functional cookies - Improvement of functionality by remembering personal preferences and settings etc.
☐ Statistics – Anonymous collection of data related to customer interaction
☐ Marketing – Tracking of users across websites to display relevant ads etc
☐ Other, please elaborate

Is the user offered functionality to disable cookies?

◯ No (only possible in web browser by the user)
◯ Yes, functionality available at company web pages

Bibliography

[1] The European Union EU. General data protection regulation. https://gdpr-info.eu/, 2016.

[2] PCI Security Standards Council. Pci security standard. https://www.pcisecuritystandards.org/, 2021.

[3] The European Union. Directive on privacy and electronic communications. https://eur-lex.europa.eu/, 2002.

[4] Justis og beredskapsdepartementet. Lov om behandling av personopplysninger. https://www.iso.orhttps://lovdata.no/dokument/NL/lov/2018-06-15-38, 2018.

[5] Datatilsynet. Høyringsfråsegn - ny lov om pengespel. https://http://www.regjeringen.no/no/id4/, 2020.

[6] The Information Commissioner's Office. https://ico.org.uk/, 2020.

[7] U.S. Department of Commerce. General data protection regulation. https://www.privacyshield.gov/welcome, 2015.

[8] European Data Protection Supervisor. Case c-311/18 data protection commissioner v facebook ireland ltd and maximilian schrems ("schrems ii"). https://edps.europa.eu/, 2020.

[9] ISO International Organization for Standardization. Iso/iec 27001 information security management. https://www.iso.org/, 2013.

[10] National Instutite of Standardization and Technology. An introduction to information security. https:https://csrc.nist.gov/, 2018.

[11] ISO International Organization for Standardization. Information technology security techniques. https://www.iso.org/, 2018.

[12] ISO International Organization for Standardization. Security techniques — extension to iso/iec 27001 and iso/iec 27002 for privacy information management — requirements and guidelines. https://www.iso.org/, 2019.

[13] The European Union - EU. Directive on privacy and electronic communications. https://eur-lex.europa.eu/, 2019.

[14] Den norske regjeringen. Lov om elektronisk kommunikasjon (ekomloven). //https://lovdata.no/, 2003.

[15] World Lottery association. Wla scs - world lottery association security and control standard. https://www.world-lotteries.org/, 2020.

[16] Louis D. Brandeis Samuel D. Warren. The rights to privacy. *Harvard Law Review*, 4(5), 1890.

[17] Alan Westin. *Privacy and freedom*. London, Bodley Head, 1970.

[18] Charles Fried. Privacy. *The Yale Law Journal Company, Inc*, 3(77), 1968.

[19] Tjerk Timan Ivan Škorvánek Tomislav Chokrevski Bert-Jaap Koops, Bryce Clayton Newell and Maša Galič. A typology of privacy.

[20] Autralian law enforcement committee. The meaning of privacy. https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/1-introduction-to-the-inquiry-5/the-meaning-of-privacy/, 2010.

[21] World Legal Information Institute. Models of privacy protection. http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Models.html, 2006.

[22] Iab europe transparency and consent framework policies. https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/, 2020.

[23] Heng Xu H. Jeff Smith, Tmara Dinev. Information privacy research:an interdisiplinary review. http://www.researchgate.net, 2011.

[24] Patricia Warrington Mary Ann Eastlicka, Sherry L. Lotza. Understanding online b-to-c relationships: An integrated modelof privacy concerns, trust, and commitment. https://www.researchgate.net/publication/4967370_Understanding_online_B-to-C_relationships_An_integrated_model_of_privacy_concerns_trust_and_commitment, 2006.

[25] Miriam J. Metzger. *Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerceesearch:An interdisiplinary review*. 2017.

[26] Steve Werner, Moira Praxedes and Hyun-Gyu Kim. The reporting of nonresponse analyses in survey research. https://http://www.researchgate.net/, 2007.

[27] Kantar. Omdømmemålingen 2020. https://kantar.no/, 2020.

[28] Roger C. Mayer, James H. Davis and F. David Schoorman. An integrative model of organizational trust. https://makinggood.ac.nz, 1995.

[29] Maximizing the value of your data privacy investments. https://www.cisco.com/.

[30] Kelly D. Martin , Abhishek Borah and Robert W. Palmatier. A strong privacy policy can save your company millions. https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions, 2019.

[31] Ståle Pallesen, Rune Aune Mentzoni, Torbjørn Torsheim, Eilin Erevik, Helge Molde og Arne Magnus Morken . Omfang av penge- og dataspillproblemer i norge. Available at: www.uib.no, 2020.

[32] Michael Auer. Behavioural tracking and the effects of responsible gaming tools and personalized feedback in online gambling. https://http://irep.ntu.ac.uk/, 2015.

[33] Hedman, E., Ljotsson, B., Lindefors. Cognitive behavior therapy via the internet: a systematic review of applications, clinical efficacy and cost-effectiveness. https://http://www.academia.edu/, 2012.

[34] Martens, M. P., Arterberry, B. J., Takamatsu, S. K., Masters, J., Dude, K. The efficacy of a personalized feedback-only intervention for at-risk college gamblers. https://http://www.researchgate.net/, 2015.

[35] Neccton. https://www.neccton.com/, 2020.

[36] Playscan. http://www.playscan.com/.

[37] Alex Blaszczynski, Robert Ladouceur, Howard J. Shaffer . A science-based framework for responsible gambling: The reno model. https://http://link.springer.com/, 2004.

[38] Maris Bonello Mark Griffiths. Behavioural tracking, responsible gambling tools, and online voluntary self-exclusion: Implifications for problem gamblers. https://http://irep.ntu.ac.uk/, 2019.

[39] Ministry of Science Technology and innovation in Denmark. Privacy enhancing technologies. //https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf/.

[40] Thijs Veugen Milena Janic, Jan Pieter Wijbenga. Gtransparency enhancing tools (tets): an overview. https://www.academia.edu/31328255/Transparency_Enhancing_Tools_TETs_An_Overview, 2013.

[41] Hans Hedbom. A survey on transparency tools for enhancing privacy. https://www.researchgate.net/publication/251415213_Transparency_Tools, 2011.

[42] Philip Fei Wu Royal Holloway,. The privacy paradox in the context of online social networking: A self-identity perspective: Journal of the association for information science and technology. https://www.researchgate.net/, 2018.

[43] Young Min Baek. Solving the privacy paradox: A counter-argument experimental approach. https://dokumen.tips/, 2014.

[44] worsl-lotteries.org. https://www.world-lotteries.org/, 2020.

[45] Information systems audit and control association. https://www.isaca.org/, 2021.

[46] Pauld D. Leedy, Jeanne Elis Ormrod. *Practical research - Planning and Design*. 2015.

[47] Federal Court of Justice, Germany. Planet 49 case. https://curia.europa.eu, 2019.

[48] The European Union - EU. Anti-money laundering (amld v) - directive (eu) 2018/843. https://ec.europa.eu/, 2018.

[49] Rohit H. Trivedi and Thorsten Teichert. The janus-faced role of gambling flow in addiction issues. /https://www.researchgate.net/, 2017.

[50] Mark D. Griffiths Michael Auer. The use of personalized messages on wagering behavior of swedish online gamblers: An empirical study. https://www.sciencedirect.com/, 2017.

[51] The European Union - EU. Protection of persons who report breaches of union law. https://eur-lex.europa.eu/, 2019.

[52] T W O'Neill, D Marsden, C Matthis, H Raspe, A J Silman, and the European Vertebral Osteoporosis Study Group. National and regional differences in a european multicentre study of vertebral osteoporosis. https://www.reresearchgate.net/, 1995.

[53] Gerhard Schwarz. Response rates in european business tendency surveys. https:///www.oecd.org/, 2013.

[54] The Norwegian Ministry of finance. The anti-money laundering act. https://lovdata.no/, 2019.

[55] Wikipedia. Politically exposed person. https://en.wikipedia.org/wiki/Politically_exposed_person, 2020.

[56] BankID. https://www.bankid.no/, 2020.

[57] Vipps. https://www.vipps.no/, 2020.

[58] Collins P. Fong D. Ladouceur R. Nower L. Shaffer H. ... Venisse J.-L. Blaszczynski, A. Responsible gambling: General principles and minimal requirements. https://www.reserachgate.net/, 2011.

[59] Sally Melissa Gainsbury and Alex Blaszczynski. Electronic gaming machine warning messages: Information versus sel-evaluation evaluation. https://www.reserachgate.net/, 2020.

[60] Katja Frankling, Svenska Spel - Personal communication.

[61] Hugo Hesser Per Carlbring David Forsström, Markus Jansson-Fröjmark. Interviews with users of a responsible gambling tool. https://www.elsevier.com/, 2017.

[62] Den Norske Regjering. https://www.regjeringen.no/, 2020.

[63] Wikipedia. https://en.wikipedia.org/wiki/Money_laundering/, 2020.

[64] Cookieinformation. Cookie information - consent management platform. https://cookieinformation.com/, 2020.

[65] adform.com. https://site.adform.com/privacy-center/adform-cookies/, 2020.

[66] cookiedatabase.org. https://cookiedatabase.org, 2020.

[67] Facebook.com. https://www.facebook.com/policy/cookies, 2020.

[68] The Europen Union - EU. https://eur-lex.europa.eu/, 2017.

[69] The European Union. Opinion 4/2007 on the concept of personal data. https://https://ec.europa.eu/.

[70] Peter Eckersley. How unique is your web browser. https://link.springer.com/, 2010.

[71] Erik Wijmans Yinczhi Cao, Song Li. (cross-)browser fingerprinting via os and hardware level feautres. https://www.researchgate.net/, 2017.

[72] Google Support. Help center - ip anonymization (or ip masking) in google analytic's. https://support.google.com/analytics/answer/2763052?hl=en, 2021.

[73] Onetrust. https://sourceforge.net/software/product/OneTrust/, 2020.

[74] Hugo Hesser Per Carlbring David Forsström, Markus Jansson-Fröjmark. Experiences of playscan: Interviews with users of a responsible gambling tool. *https://www.elsevier.com/*, 2017.

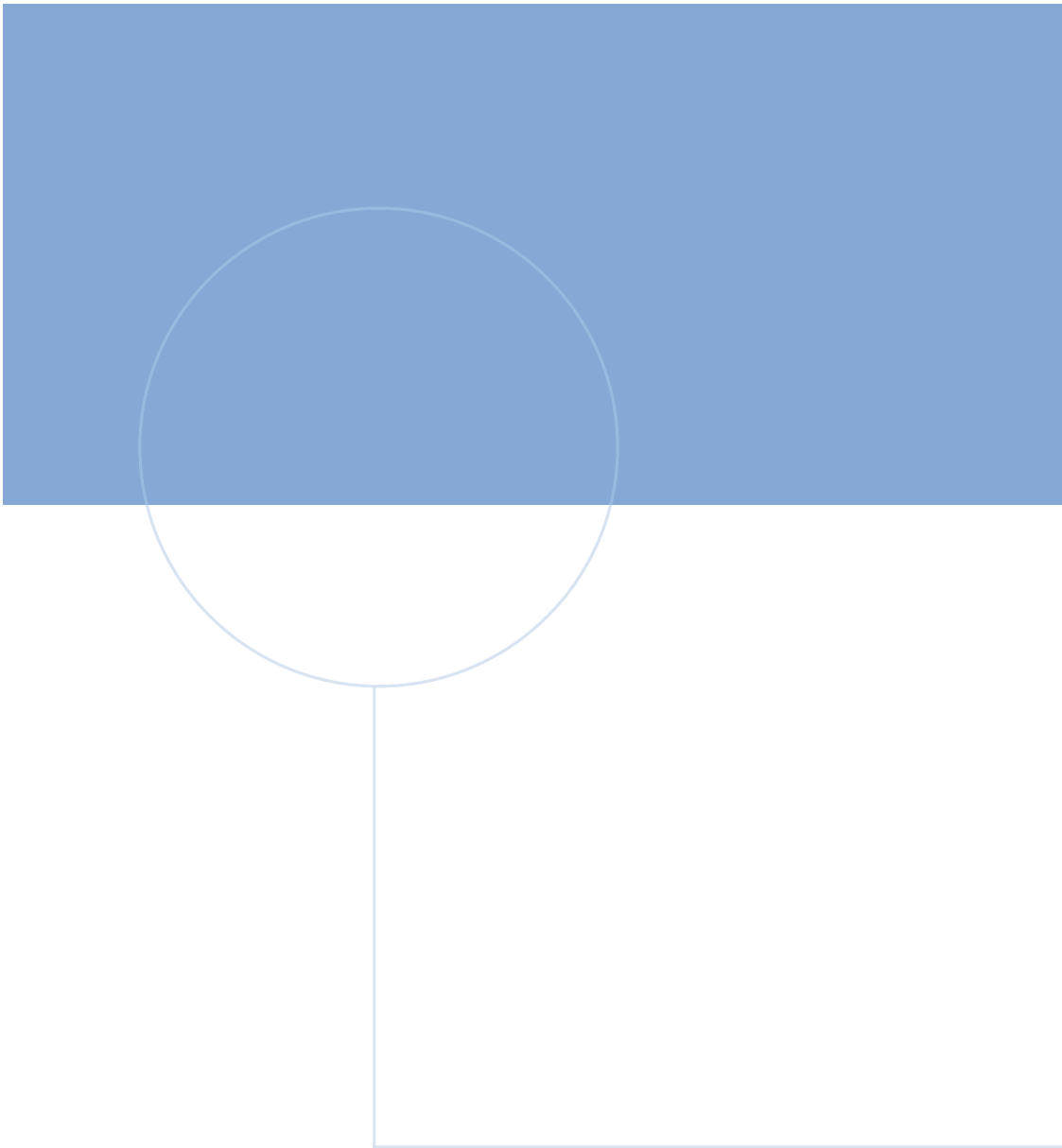
[75] IBM. Artificial intelligence (ai). https://www.ibm.com/cloud/learn/what-is-artificial-intelligence, 2021.

[76] The Technology Analysis Division of the Office of the Privacy Commissioner of Canada. Privacy enhancing technologies – a review of tools and techniques. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/, 2017.

[77] Jeanne Ellis Ormrod Paul Leedy. *Practical research*. Pearson, 2015.

[78] The European Union. The data protection directiv. https://eur-lex.europa.eu/, 1995.

[79] ISO International Organization for Standardization. Information technology — security techniques — code of practice for information security management. https://www.iso.org/, 2005.



NTNU

Kunnskap for en bedre verden